



# Mutual Evaluation Report

Anti-Money Laundering and Combating the  
Financing of Terrorism

# GERMANY

19 February 2010

Germany is a member of the Financial Action Task Force. This evaluation was conducted by the International Monetary Fund and was adopted as a third mutual evaluation by its Plenary on 19 February 2010.

© 2010 FATF/OECD and IMF. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission. Requests for permission to further disseminate, reproduce or translate all or part of this publication should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France (fax +33 1 44 30 61 37 or e-mail: [contact@fatf-gafi.org](mailto:contact@fatf-gafi.org))

## TABLE OF CONTENTS

ACRONYMS .....	6
PREFACE .....	8
EXECUTIVE SUMMARY .....	9
1. GENERAL .....	15
1.1. General Information on Germany .....	15
1.2. General Situation of Money Laundering and Financing of Terrorism.....	21
1.3. Overview of the Financial Sector.....	30
1.4. Overview of the DNFBP Sector.....	35
1.5. Overview of commercial laws and mechanisms governing legal persons and arrangements.....	37
1.6. Overview of strategy to prevent money laundering and terrorist financing.....	38
2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES.....	49
2.2. Criminalization of Terrorist Financing (SR.II) .....	66
2.3. Confiscation, freezing and seizing of proceeds of crime (R.3).....	75
2.4. Freezing of funds used for terrorist financing (SR.III) .....	86
2.5. The Financial Intelligence Unit and its Functions (R.26) .....	97
2.6. Law enforcement, prosecution and other competent authorities – the framework for the investigation and prosecution of offenses, and for confiscation and freezing (R.27, & 28).....	107
2.7. Cross-Border Declaration or Disclosure (SR.IX) .....	117
3. PREVENTIVE MEASURES – FINANCIAL INSTITUTIONS .....	130
3.1. Risk of money laundering or terrorist financing .....	132
3.2. Customer due diligence, including enhanced or reduced measures (R.5 to 8) .....	133
3.3. Third Parties and Introduced Business (R. 9) .....	148
3.4. Financial Institution Secrecy or Confidentiality (R.4).....	151
3.5. Record-keeping and wire transfer rules (R.10 & SR.VII).....	153
3.6. Monitoring of Transactions and Relationships (R.11 & 21).....	160
3.7. Suspicious Transaction Reports and Other Reporting (R.13-14, 19, 25 & SR.IV).....	164
3.8. Internal Controls, Compliance, Audit and Foreign Branches (R.15 & 22).....	174
3.9. Shell Banks (R.18) .....	180
3.10. The Supervisory and Oversight System – Competent Authorities and SROs. Role, Functions, Duties, and Powers (Including Sanctions) (R. 23, 29, 17 & 25).....	181
3.11. Money or Value Transfer Services (SR.VI) .....	204
4. PREVENTIVE MEASURES – DESIGNATED NONFINANCIAL BUSINESSES AND PROFESSIONS .....	208
4.1. Customer Due Diligence and Record keeping (R.12).....	208
4.2. Suspicious Transaction Reporting (R.16) .....	223
4.3. Regulation, Supervision, and Monitoring (R.24-25).....	230

4.4.	Other Non-Financial Businesses and Professions – Modern-Secure Transaction Techniques	239
5.	LEGAL PERSONS AND ARRANGEMENTS AND NON-PROFIT ORGANIZATIONS	244
5.1.	Legal Persons – Access to Beneficial Ownership and Control Information (R.33)	244
5.2.	Legal Arrangements — Access to Beneficial Ownership and Control Information (R.34)	250
5.3.	Non-Profit Organizations (SR.VIII)	253
6.	NATIONAL AND INTERNATIONAL COOPERATION	263
6.1.	National Cooperation and Coordination (R. 31 & R. 32)	263
6.2.	The Conventions and UN Special Resolutions (R.35 & SR.I)	266
6.3.	Mutual Legal Assistance (R.36-38, SR.V)	269
6.4.	Extradition (R.37, 39, SR.V)	286
6.5.	Other Forms of International Cooperation (R.40 & SR.V)	290
7.	OTHER ISSUES	300
7.1.	Resources and Statistics	300
7.2.	Other relevant AML/CFT Measures or Issues	300

#### STATISTICAL TABLES

Statistical Table 1: Key Information about Germany–2008	17
Statistical Table 2: Germany Governance Indicators	20
Statistical Table 4: Selected Crime Statistics	22
Statistical Table 5: Some estimates of potential proceeds of crime in Germany(a)	23
Statistical Table 6: Summary Statistics on Organized Crime in Germany	24
Statistical Table 8: Prosecutions and Convictions for main predicate crimes mentioned in STR reports	27
Statistical Table 9: Financial Activity by Type of Financial Institution	32
Statistical Table 10: Foreign Financial Institutions, 2008	35
Statistical Table 11: Structure of DNFBP Sector, 2008	37
Statistical Table 12: Imprisonment or youth custody sanctions for those convicted of offenses pursuant to	58
Statistical Table 13: Convictions for ML	61
Statistical Table 14: Acquittals on ML charges by Section	62
Statistical Table 15: ML Conviction Statistics for Selected Countries	63
Statistical Table 16: Investigations Conducted for Combating Terrorism (including financial	72
Statistical Table 17: Total Assets Forfeited and Confiscated 2004-2007	81
Statistical Table 18: Total Assets Forfeited or Confiscated in Relation to Single Offenses	82
Statistical Table 19: Selected Comparative Information for Assets frozen, restrained, seized,	83
Statistical Table 20: STRs filed by the Financial Sector	169
Statistical Table 21: AML/CFT Risk Profiles of Credit institutions on the basis of the evaluation of reports	194
Statistical Table 22: AML/CFT Risk Profiles of money remittance services and currency	194
Statistical Table 23: AML/CFT Risk Profiles of financial services institutions (other than those	194
Statistical Table 24: AML/CFT Risk Profiles of insurance undertakings (life insurance and	195
Statistical Table 25: DNFBPs and legislation regulating them	209
Statistical Table 26: STRs Filed by DNFBPs	228
Statistical Table 27: Number of online accounts according to the statistics of the <i>Deutsche</i>	240
Statistical Table 28: Treaties of the Council of Europe	271
Statistical Table 29: Multilateral Treaties of the European Union	274
Statistical Table 30: Multilateral Treaties of the United Nations	274

---

Statistical Table 31: Bilateral Extradition Treaties between the Federal Republic of Germany and .....	275
Statistical Table 32: Bilateral Mutual Legal Assistance Treaties between the Federal Republic of .....	276
Statistical Table 33: Extradition Requests from Other Countries .....	288

## FIGURES

Figure 1: High denomination banknotes in circulation in the EU .....	18
Figure 2: Crime Rates in the "Länder" of Germany .....	25
Figure 3. Profile of Terrorist Incidents in Germany since 1970.....	29

## ACRONYMS

AML	Anti-Money Laundering
BaFin	Federal Financial Supervisory Authority ( <i>Bundesanstalt für Finanzdienstleistungsaufsicht</i> )
BKA	Federal Criminal Police Office ( <i>Bundeskriminalamt</i> )
BGBI	Federal Law Gazette
BMI	Federal Ministry of Interior
BWG	Banking Act ( <i>Bankwesengesetz</i> )
CARIN	Camden Asset recovery Inter-Agency Network
CC	Criminal Code
CAA	Customs Administration Act
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CIS	Community of Independent States
CPC	Criminal Procedures Code
DNFBP	Designated Non-Financial Businesses and Professions
DSt	Disciplinary Statute for lawyers and lawyer-candidates ( <i>Disziplinarstatut</i> )
EC	European Commission
ECB	European Central Bank
EEA	European Economic Area
EU	European Union
EUR	Euro
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSAP	Financial Sector Assessment Program
FT	Financing of terrorism
GDP	Gross Domestic Product
GDV	Federal Association of Insurance Companies ( <i>Gesamtverband der Deutschen Versicherungswirtschaft</i> )
INZOLL	Customs Investigation Service's information system
KfW	Development Loan Corporation ( <i>Kreditanstalt fuer Wiederaufbau</i> )
LEA	Law enforcement authority
LEG	Legal Department of the IMF
LKA	Land Police ( <i>Landeskriminalamt</i> )
ML	Money Laundering
MLA	Mutual Legal Assistance
MLPG	Money Laundering Prevention Group, part of the BaFin
MoET	Federal Ministry of Economics and Technology
MoF	Federal Ministry of Finance
MoFA	Federal Ministry of Foreign Affairs
MoJ	Federal Ministry of Justice
MOU	Memorandum of Understanding
MVT	Money Value Transfer
n.a.	Not Applicable

N/A	Not Available
NCCT	Non Cooperative Countries and Territories
NPO	Nonprofit organization
OECD	Organization for Economic Development and Cooperation
OFAC	U.S. Treasury Office of Foreign Assets Control
PEP	Politically-Exposed Person
ROSC	Report on Observance of Standards and Codes
SRO	Self-Regulatory Organization
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider
TF	Terrorist Financing
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
UNSCR	United Nations Security Council Resolution
ZKA	Central Association of the German Banking Industry ( <i>Zentraler Kreditausschuss</i> )

## PREFACE

This assessment of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of the Federal Republic of Germany is based on the Forty Recommendations 2003 and the Nine Special Recommendations on Terrorist Financing 2001 (FATF 40+9 Recommendations) of the Financial Action Task Force (FATF), and was prepared using the AML/CFT assessment Methodology 2004, as updated from time to time. The assessment team considered all the materials supplied by the authorities, the information obtained on site during their mission from May 15 to June 5, 2009, and other verifiable information subsequently provided by the authorities. During the mission, the assessment team met with officials and representatives of all relevant government agencies and the private sector. A list of the bodies met is set out in Annex 1 to the detailed assessment report.

A team of assessors composed of staff of the International Monetary Fund (IMF) and six expert(s) acting under the supervision of the IMF conducted the assessment. The assessment team consisted of: Steve Dawe, Senior Financial Sector Expert (Legal Department (LEG), team leader); Nadine Schwarz, Counsel, (LEG, deputy team leader); and the following consultants under LEG supervision: Richard Chalmers, U.K., and Nicolas Burbidge, Canada (both financial sector experts), Horst Intscher, Canada (law enforcement expert), John Abbott, U.S.A. (expert on Designated Non-Financial Businesses and Professions–DNFBPs) and, Mariano Federici, Argentina (legal expert).<sup>1</sup> The assessors reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter and punish money laundering (ML) and the financing of terrorism (FT) through financial institutions and DNFBPs. The assessors also examined the capacity, implementation, and effectiveness of all these systems.

This report provides a summary of the AML/CFT measures in place in Germany at the time of the mission or shortly thereafter. It describes and analyzes those measures, sets out Germany's levels of compliance with the FATF 40+9 Recommendations (see Table 1), and provides recommendations on how certain aspects of the system could be strengthened (see Table 2).

The assessors would like to express their gratitude to the German authorities for their cooperation throughout the assessment mission.

---

<sup>1</sup> The assessment team was also accompanied by Giovanni Francesco D'eccelesiis, Italy (observer), and Jocelyn C. Gabriel, Administrative Assistant, Legal Department, IMF.



## EXECUTIVE SUMMARY

### Background information

1. This report summarises the anti-money laundering and counter-terrorist financing measures (AML/CFT) that were in place in Germany at the time of the on-site visit (15 May – 5 June 2009) and immediately thereafter. It describes and analyses these measures and offers recommendations on how to strengthen certain aspects of the system. It also assesses Germany's level of compliance with the 40+9 Recommendations of the Financial Action Task Force (FATF).

### Key Findings

2. **Germany has introduced a number of measures in recent years to strengthen its anti-money laundering and combating the financing of terrorism (AML/CFT) regime.** Germany has generated a relatively large number of prosecutions for money laundering (ML) and of orders to confiscate assets. These achievements occurred even though Germany has shortcomings identified in this assessment against the Financial Action Task Force (FATF) 40+ 9 Recommendations.

3. **Many indicators suggest that Germany is susceptible to money laundering (ML) and terrorist financing (TF) including because of its large economy and financial center, as well as its strategic location in Europe and its strong international linkages.** Substantial proceeds of crime are generated in Germany, presently estimated to be EUR 40 to EUR 60 billion (approximately USD 60–80 billion), inclusive of tax evasion, annually. Terrorists have carried out terrorist acts in Germany and in other nations after being based in Germany. Germany is also estimated to have a large informal sector (> EUR 400 billion or >USD 560 billion) and the use of cash is reportedly high. Germany's currency is the Euro (EUR), which is used widely across Europe, thus making it attractive to organized criminals and tax evaders. Key factors that may reduce Germany's risk profile for ML include its strong legal tradition, the rule of law, its political environment, and having an effective single financial regulator.

4. **The core elements of Germany's AML/CFT regime are established in the German Criminal Code (CC), which contains the ML and TF offenses; the Money Laundering Act (AML Act); and the sector-specific laws such as the Banking Act.** The AML Act established Germany's financial intelligence unit (FIU) within the Federal Criminal Police Office (BKA), imposes customer due diligence (CDD) obligations on a wide range of financial institutions (FIs), and requires these FIs to submit suspicious transaction reports (STRs) to the competent authorities. The Act was most recently amended in August 2008, when Germany transposed the third European Union (EU) Money Laundering Directive,<sup>2</sup> and its Implementing Directive,<sup>3</sup> into national law.

---

<sup>2</sup> Directive 2005/60/EC of the European Parliament and of the Council October 26, 2005 on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing (third EU Directive).

<sup>3</sup> Commission Directive 2006/70/EC of August 1, 2006.

5. **The AML/CFT framework is not fully in line with the FATF Recommendations.** There are weaknesses in the legal framework and in sanctioning for noncompliance with AML/CFT requirements. The recommendations to address these include:

- amending the CC to: criminalize (i) ML in a way that covers all serious predicate offenses, and (ii) TF in a way fully consistent with international standards;
- amending the AML Act to: (i) improve preventive measures notably by imposing a reporting obligation based on suspicion rather than knowledge and that relates to the proceeds of criminal activity; and (ii) clearly establish that the FIU should carry out more of the core functions of an FIU as contemplated by the FATF standard;
- fully and effectively implementing the UN Security Council Resolutions (UNSCRs) on TF;
- applying sanctioning powers more effectively for breaches of AML/CFT obligations;
- strengthening the effective implementation of AML/CFT obligations imposed on designated non-financial businesses and professions (DNFBPs); and
- improving the collection of statistics and the provision of guidance and feedback to FIs.

#### **Legal Systems and Related Institutional Measures**

6. **The principal AML provisions of the CC are largely consistent with the FATF standard, but there are some technical deficiencies.** In particular, two of the FATF-designated categories of offenses are not predicates for ML, and the ML offense itself cannot be applied to persons convicted of a predicate offense (without the assessors being convinced that this was justified by fundamental principles of German law). In addition, legal persons are not subject to criminal liability due to fundamental principles of German law, although those involved in an ML criminal offense may be subject to administrative fines imposed by the criminal courts.

7. **Germany's criminal justice system appears to achieve effective outcomes for dealing with profit motivated crimes; however, the ML offense is not the primary tool used for this purpose.** German courts obtain more than 300 ML convictions yearly, but many are for less serious ML conduct. Serious ML conduct (for example, involving organized crime) is usually pursued via predicate offenses that carry more severe sanctions than the ML offense. The high burden of proof required to show that proceeds relate to a predicate crime and the inability to convict for ML, persons convicted of the predicate, are also reasons cited for not pursuing the ML offense.

8. **In August 2009, Germany enhanced its CFT requirements by criminalizing the financing of terrorist acts and individual terrorists, but technical deficiencies still remain.** The financing of terrorist organizations was already criminalized and all three CTF offenses are predicates for ML. However, they are not fully consistent with the FATF standard because, *inter alia*, they do not cover all offenses designated under the UN TF Convention; a "terrorist act" does not cover serious bodily injuries; and "funds" must, in some cases, be "not merely insubstantial." Poor statistics meant that effective implementation of TF offenses could not be established.

9. **German authorities regularly use a broad range of legal procedures to seize, confiscate, and forfeit property, but they confiscate and forfeit a lot less property than the courts issue orders for.** The procedures apply to all criminal offenses, including ML and TF and to property that is used or

intended to be used for carrying out offenses. The way that professional secrecy is interpreted by some professions is a limitation on the ability of law enforcement authorities (LEAs) to locate and trace property.

10. **Terrorist funds or other assets may be frozen, without delay, largely in line with relevant UNSCRs.** However, some requirements to freeze do not apply to all EU residents and some apply, as far as certain EU-residents are concerned, only to funds, not other assets.

11. **The AML Act requires reporting entities to submit STRs to the relevant *Land* police or prosecutorial body with a copy to the FIU, which is the national center for receiving STRs.** The reporting system has been structured this way because, under the German Constitution, states (*Länder*) are responsible for policing and law enforcement. The FIU's mandate includes supporting the Federal and *Länder* LEAs in the prevention and prosecution of ML and TF.

12. **In practice, the processing and analysis of STRs is split between the *Länder* LEAs and the FIU, with the FIU carrying out only limited case-specific analysis.** The *Land* recipient of the STR establishes whether there are grounds to undertake a full investigation. The FIU contributes modestly to this process, with *Länder* police and prosecutorial officials valuing mainly its access to information from foreign FIUs. The FIU checks STRs against its own database of all previous STRs and searches other BKA databases. It is solely responsible for requesting or exchanging information with foreign FIUs. Information yielded by these processes is forwarded to the *Land* LEA that received the STR. The FIU does not, as such, disseminate disclosures of STRs concerning suspected ML or TF activities to the investigative bodies.

13. **The FIU focuses its analytic work on the elaboration of patterns and trends, which it disseminates to reporting entities and investigative bodies.** It maintains statistics on a range of ML and TF matters, publishes an annual report and other documents, and informs reporting entities and LEAs of ML and TF typologies and methods. Overall, while the FIU discharges its legal mandate, it does not carry out fully all the FIU functions required under the standard.

14. **LEAs have powers necessary to carry out their ML and TF investigations and are generally effective.** The authorities that investigate and prosecute ML are mainly the *Länder* police and prosecutors, and for TF also the BKA. For ML, they generally favor pursuing predicate offenses due to the nature of the ML offense.

15. **Germany has two, largely effective, regimes in place to monitor cross-border physical transportation of currency and negotiable instruments of EUR 10 000 or more.** One applies to movements between Germany and non-EU countries and requires travelers to complete a declaration; and the other applies to movements within the EU and requires travelers to disclose information if asked. The Customs Administration implements both regimes, has broad powers, and operates using a risk-based approach. Data from the regimes are, in practice, accessible by Customs, some *Länder* LEAs, and the BKA, including the FIU; however, much of the data are stored for one year only, considerably diminishing its utility for identifying cash couriers, trends, or typologies. More needs to be done to inform travellers entering the EU through German airports of their declaration obligation.

#### **Preventive Measures – Financial Institutions**

16. **The AML Act applies CDD and record-keeping requirements to credit institutions, financial services institutions, financial enterprises, insurance companies, insurance intermediaries and investment companies, as well as a broad range of nonfinancial sector persons or entities.** The scope of the activities of all these entities covers the vast majority of the financial activities listed under the FATF standard. The amendments of the AML Act in 2008 strengthened the existing requirements and explicitly introduced a risk-based approach to the implementation of CDD measures (although some

elements of that approach were already in place). The preventive measures apply equally to all persons and entities subject to the Act. Additional CDD provisions have also been laid out in sector-specific laws.

17. **Notwithstanding the generally adequate framework of preventive measures, the structure of the measures in specific areas is problematic.** These include: the very broad CDD exemptions granted with respect to specified “low-risk” customers, which appear to conflict with some basic monitoring and record-keeping obligations; the treatment of all the EU/European Economic Area (EEA) member states and jurisdictions on the EU’s third country equivalence list as a single-risk category when determining certain low-risk scenarios; the treatment of the EU/EEA as a single domestic market in terms of correspondent banking obligations; and the concept of what constitutes “senior management” in relation to the approvals processes for politically-exposed persons (PEPs) and correspondent banking relationships.

18. **One area of particular concern is the verification of beneficial ownership** (including the determination of whether a customer is a PEP). The measures in place do not fully conform to the FATF standard; and there appears to be a wide variety of interpretations among individual institutions of what is required. The BaFin issued a circular clarifying some aspects of the expected approach in July 2009, and this may assist for the future.

19. **Institutions generally retain records for ten years pursuant to commercial law requirements, but may have inadequate records on low-risk customers.** Institutions are exempted from several key CDD components in low-risk situations, thereby bringing into question what information they would record and have available for the authorities about low-risk customers.

20. **Institutions implement effectively EU Regulation 1781/2006 on wire transfers which meets the requirements of the FATF standard.**

21. **The statutory provisions relating to the monitoring of transactions, including transactions with persons in countries that do not or insufficiently apply the FATF standard are generally weak,** but specific guidance has been provided to institutions in the form of the BaFin circulars, which highlight weaknesses in the AML/CFT regimes of other countries, typically (but not exclusively) in line with the public statements made by the FATF.

22. **STR reporting is well established, but the reporting obligation fails to meet the FATF standard in several key areas.** The “evidential” basis upon which STRs are to be filed is significantly higher than the FATF concept of “suspects or has reasonable grounds to suspect.” The linkage of the obligation to the ML or TF offenses also sets a more restricted trigger for reporting than is envisaged by FATF with the “proceeds of criminal activity.” Moreover, filing the reports directly with *Länder* LEAs means that STRs are treated as criminal complaints. In addition, certain limitations in the range and definitions of the predicate offenses narrow further the scope of the reporting obligation. Overall, these factors discourage reporting and result in comparatively fewer STRs being filed in Germany than in other countries, thus denying the FIU and LEAs access to a wider intelligence base.

23. **Some internal control requirements are in place, but these need to be improved and implemented more effectively by financial institutions.** These requirements do not apply to the more than 72 000 insurance intermediaries. The legislative requirements for the role of compliance officers need to be broadened and the officers’ oversight responsibilities strengthened. The obligation to train staff is limited and there is no obligation for FIs to put in place screening procedures to ensure high standards when hiring them.

24. **Shell banks are effectively prohibited from operating in Germany.** German banks and insurers operating outside Germany are subject to an obligation to implement AML/CFT measures at least

equivalent to German requirements. However, there are no explicit provisions requiring attention to equivalency in EU or EEA states that do not or insufficiently apply the FATF Recommendations. Germany prohibits banking entities from operating in non EU or EEA countries where measures consistent with German requirements cannot be implemented. However, there are no obligations imposed at all regarding investment sector operations outside Germany, and German FIs are not required to pay attention to their operations in countries with weak AML/CFT regimes.

25. **The BaFin is responsible for most FI supervision in Germany, has adequate AML/CFT supervisory powers, and uses a risk-based approach for its supervision.** The AML/CFT supervisory arrangements rely heavily on a statutory regime of annual external audits. At the time of the on-site visit, the methodology for these audits had not been updated to reflect the 2008 AML Act, and there were some doubts about the quality of audit reports for some cooperative banks. Although the number of on-site inspections is low, significant risk-based off-site monitoring and analysis enables the auditors and the BaFin to focus on-site work on higher-risk entities. Germany is moving to, but has not yet fully implemented, a system of private sector issued AML/CFT guidance approved by the BaFin. The BaFin abrogated most of its previous guidance as a result of the new AML Act, but nonetheless states that it continues to apply supervisory principles set out in the abrogated guidance when those principles are in line with the new laws and the private sector guidance. This has caused confusion in parts of the financial sector. *Länder* authorities seem generally unfamiliar with their AML/CFT supervisory responsibilities for insurance intermediaries and apply insufficient resources to supervise them. Administrative fines are not available to sanction failure to comply with all AML/CFT requirements due to the constitutional principle of specificity. Moreover, the fines that are available are neither proportionate nor dissuasive, and are not applied effectively.

26. **The money or value transfer service (MVTs) sector is subject to AML/CFT requirements under the Banking Act and is supervised by the BaFin.** There are about 40 licensed MVTs operators in Germany.

### Preventive Measures – DNFBPs

27. **The AML Act imposes AML/CFT requirements on lawyers, patent attorneys, notaries, legal advisers, auditors, chartered accountants, tax advisers, tax agents, trust and company service providers (TCSPs), real estate agents, persons trading in goods, and gambling casinos, but implementation by these businesses and professions is uneven.** The requirements are essentially identical to those imposed on FIs. Supervisory arrangements have been established for most of these businesses and professions. There is no systematic implementation of AML/CFT measures by, or supervision of, real estate agents, independent TCSPs, dealers in precious metals and dealers in precious stones. The legal and accounting professions are generally familiar with their obligations but lack awareness of their ML and TF vulnerabilities. They are also subject to strict professional secrecy obligations which contribute to a low level of reporting of suspicious transactions and complicate cooperation with investigative authorities. Overall, the effectiveness of implementation in the DNFBP sector is difficult to ascertain.

### Legal Persons and Arrangements and Non-Profit Organizations

28. **The extent of information available on the ownership and control of German legal persons varies greatly by type of legal entity.** The main information sources are public registers, but they do not always include information on the beneficial ownership and control of the legal entities. The information available is considerably limited in the case of nonlisted stock corporations that issue bearer shares, and is close to nonexistent in the case of private foundations.

29. **The *Treuhand* is a commonly used legal arrangement in Germany but disclosure obligations in place are insufficient to ensure transparency of the beneficial ownership and control of such arrangements.**

30. **Germany prevents abuse of the non-profit organization (NPO) sector for TF purposes through (a) measures to ensure the transparency of the sector; and (b) targeted, intelligence-driven monitoring, surveillance, investigation, and suppression of extremists and terrorist activities.** A formal review of the NPO sector has been undertaken. Legislative and regulatory provisions have been introduced to enhance responsibilities and oversight of NPOs. Enforcement actions have been taken under the new provisions. Outreach activities to promote awareness of TF vulnerabilities among NPOs have also been undertaken.

### **National and International Cooperation**

31. **The framework in place enables the provision of comprehensive and timely mutual legal assistance (MLA) and extradition.** While no material obstacles were identified in this area, assessors were unable to establish fully whether MLA is being provided in an effective manner due to the absence of statistics. However, Germany has a solid system in place for extradition and grants a high percentage of requests in a timely manner. In addition, the authorities appear to be providing a wide range of international administrative cooperation with their foreign counterparts except in relation to nonfinancial businesses and professions.

### **Other Issues**

32. **The BaFin operates an automated account access system, which is an efficient tool that complements AML/CFT efforts.** The system enables the BaFin, upon request, to provide certain authorities (including LEAs) with information about whether a particular person (natural or legal) has a bank or safe custody account with institutions operating in Germany.



## 1. GENERAL

### 1.1. General Information on Germany

33. Germany, officially the Federal Republic of Germany (in German: Bundesrepublik Deutschland), is a large country in the center of Europe. The territory of Germany covers 357 092 square kilometers. German is the language spoken in Germany. With over 82 million inhabitants, it has the largest population of any member state of the European Union (EU)<sup>4</sup> and the country is home to the third-largest number of international migrants worldwide (more than 10 million). A high proportion of Germany's population lives in urban areas (74%).

34. Germany has 3 621 kilometers (km) of land borders and 2 389 km of coastline. The lengths of Germany's borders with its neighbors are: in the north, Denmark (68 km); to the east, Poland (456 km) and Czech Republic (646 km); to the south, Austria (784 km) and Switzerland (334 km); and to the west France (451 km), Luxembourg (138 km), Belgium (167 km) and the Netherlands (577 km). The coastal boundaries to the north are to the North Sea, and the Baltic Sea.

35. Germany is strategically located in the center of the Schengen zone — a group of European countries with a combined population of approximately 400 million people, covering more than 4 million square kilometers, and with a combined GDP of approximately EUR 13.5 trillion (USD 18.8 trillion ) which have abolished the need for road, rail and air passengers of Schengen zone countries or from other countries who have been issued Schengen visas to have their identity checked when crossing borders between Schengen zone countries.<sup>5</sup> In addition, the EU has abolished not only border controls at internal borders, but also customs controls for the administrative processing of goods at internal borders.

<sup>4</sup> The EU members comprise: Austria, Belgium, Bulgaria, Cyprus (excluding Northern Cyprus, UN buffer zone, and U.K. Sovereign Base Areas), Czech Republic, Denmark(excluding Faroe Islands and Greenland), Estonia, Finland (including Åland Islands), France (including French Guiana, Guadeloupe, Martinique and Réunion, but excluding New Caledonia, Mayotte, French Polynesia, Saint Barthélemy, Saint Martin, Saint Pierre & Miquelon, Territory of the French Southern and Antarctic Lands, and Wallis and Futuna), Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands (excluding Aruba and Netherlands Antilles), Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom (including Gibraltar, but excluding Akrotiri and Dhekelia, Anguilla, British Antarctic Territory, Bermuda, Cayman Islands, Falkland Islands, Guernsey, British Indian Ocean Territory, Jersey, Isle of Man, Montserrat, Pitcairn Islands, Saint Helena, South Georgia and the South Sandwich Islands, Turks and Caicos Islands, and the British Virgin Islands).

<sup>5</sup> The countries comprise: Austria, Belgium, Czech Republic, Denmark (excluding Greenland and Faroe Islands); Estonia, Finland, France (including Monaco, but excluding all overseas departments and territories); Germany, Greece (excluding Mount Athos), Hungary, Iceland, Ireland (police and judicial cooperation only); Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands (excluding Aruba and Netherlands Antilles), Norway (excluding Svalbard), Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom (police and judicial cooperation only - including Gibraltar but excluding Guernsey, Isle of Man, Jersey and all overseas territories outside of Europe). In addition, the following countries have opted into the zone but have yet to implement the requirements to be full members: Bulgaria, Cyprus, Liechtenstein and Romania.

36. Germany is a federal, parliamentary, representative democratic republic of sixteen states (*Land*, plural *Länder*). The capital and largest city is Berlin. Germany is a member of the United Nations, NATO, G7, G8, G20, EU, FATF, and OECD.

37. The German political system operates under a framework laid out in the 1949 constitutional document known as the Basic Law (*Grundgesetz, GG*). The Federal Chancellor (*Bundeskanzler*) is the head of government and exercises executive power, similar to the role of a prime minister in other parliamentary democracies. Federal legislative power is vested in the Bundestag and Bundesrat, which together form a unique type of legislative body. The Bundestag is elected through direct elections, but proportional representation also applies. The members of the Bundesrat represent the governments of the sixteen *Länder*. The Federal President (*Bundespräsident*) is the head of state, invested primarily with representative responsibilities and powers.

38. An important element of the German legal landscape is that legislative power is divided between the federation and the *Länder*. The Basic Law presumes that all legislative power remains at the *Länder* level unless otherwise designated by the Basic Law itself. Any federal law overrides *Länder* law if the legislative power lies at the federal level.

39. Germany has a civil or statute-law system that is based on Roman law with some references to Germanic law. Germany's judiciary is independent from the executive and the legislative branches. Federal law delineates the structure of the judiciary, but the administration of most courts is regulated by *Land* law, meaning at the level of one of the sixteen states. The *Länder* are responsible for the lower levels of the court system; only the highest appellate courts operate at the federal level. Each of the *Länder* has its own constitutional court. The local courts (*Amtsgerichte*), regional courts (*Landgerichte*) and the higher regional courts (*Oberlandesgerichte*) are *Länder* courts of general jurisdiction. They have competence irrespective of whether the action is based on federal or *Länder* law. The Federal Court of Justice is the highest court in Germany having jurisdiction for matters under civil and criminal law. Its task is to safeguard legal uniformity through the clarification of fundamental questions of law and the development of law. In criminal cases, the Federal Court of Justice rules on appeals on points of law filed regarding judgments passed by the regional courts and the higher regional courts of first instance. Its competence includes, inter alia, so-called "capital" crimes, which are tried at the regional courts by the criminal divisions for grave offenses, and all other serious criminal offenses, provided that at the time the indictment was brought before the regional court, the public prosecutor's office could expect a prison sentence of more than four years, confinement in a psychiatric hospital or the imposition of preventive detention. The Federal Court of Justice also is the appellate court for proceedings on all crimes against the state. At first instance, the indictment will be brought before the division of a regional court competent for crimes against the state or, as in cases involving terrorist organizations, before the criminal division of a higher regional court. The Federal Constitutional Court (*Bundesverfassungsgericht*), located in Karlsruhe, is the supreme court in Germany responsible for constitutional matters, and has the power of judicial review. It acts as the highest legal authority and ensures that legislative and judicial practices conform with the Basic Law. It acts independently of the other state bodies, but cannot act on its own behalf.

40. A core element of the German constitution is the principle of *Rechtsstaat* according to Article 20 of the Basic Law. In a *Rechtsstaat*, the power of the state is limited in order to protect citizens from the arbitrary exercise of authority. It is a government based on the rule of law, in which citizens are guaranteed equality and government decisions may be challenged in court. The constitutional limit on the power of the state is an important foundation underpinning and explaining many aspects of the German AML/CFT regime.



### General information on the economy

41. Germany is the largest national economy in Europe, and the third largest by nominal GDP in the world. The service sector contributes just under 70% of total GDP, industry (including construction) 30.3%, and agriculture 0.9%. Most of the country's products are in engineering, especially in automobiles, machinery, metals, and chemical goods. Key information about the German economy is set out in Statistical Table 1.

Statistical Table 1: Key Information about Germany–2008			
		USD	World Rank if known <sup>6</sup>
Nominal Gross Domestic Product (GDP)	EUR 2 636 billion	3 668 billion	3 <sup>rd</sup>
GDP per capita	EUR 32 090	44 660	19th
Total General Government Expenditure	EUR 1 094 billion	1 523 billion	
Annual Tax Revenues	EUR 561 billion	781 billion	
Official Unemployment – 7.79%	3 163 330	n.a.	
Estimated Shadow Economy – 15.3% of GDP <sup>7</sup>	EUR 403 billion	561 billion	4th
<b>Trade:</b>			
Exports (f.o.b.)	EUR 1 054 billion	1 467 billion	1 <sup>st</sup>
Imports (c.i.f.)	EUR 867 billion	1 206 billion	
<b>Financial Sector:</b>			
Total Financial Sector Assets <sup>8</sup>	EUR 8 124 billion	11,306 billion	
Deposits in Depository Corporations	EUR 3 195 billion	4,702 billion	
Banks' claims on non-residents (e.g. loans to non-residents)	EUR 2 436 billion	3,390 billion	
Banks' liabilities to non-residents (e.g. non-resident deposits)	EUR 1 311 billion	1 825 billion	
Insurance and financial services provided to non-residents	EUR 13 billion	18 billion	
Value of Stocks Traded	EUR 2 222 billion	3 093 billion	6th
Value of transactions settled by interbank funds transfer systems	EUR 231 trillion	321 trillion	3rd
SWIFT messages send by financial institutions annually	326 million	n.a.	3rd
SWIFT messages received by financial institutions annually	289 million	n.a.	3rd
Total SWIFT messages sent and received internationally	616 million	n.a.	3rd

42. Germany is a member state of the EU and part of its single market. Germany uses the common European currency, the Euro (EUR), and its monetary policy is set by the European Central Bank (ECB) in

<sup>6</sup> Based on absolute numbers rather than proportion of GDP or other comparator.

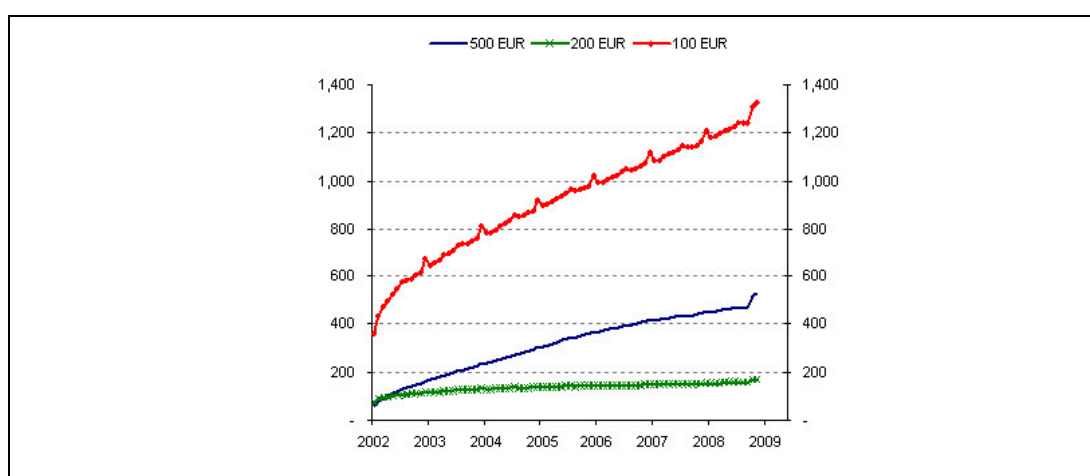
<sup>7</sup> Schneider, Friedrich. "Shadow Economies and Corruption All Over the World: What Do We Really Know?" Economics Discussion Paper No. 2007–09 (2007).

<sup>8</sup> Figure is for banking sector only, other data unavailable.

Frankfurt. Germany, through the ECB, operates a floating exchange rate regime. Germany does not have foreign exchange controls.

43. The Euro is the largest currency on issue in the world, with EUR 785 billion (USD 1 092 billion) in circulation as of December 31, 2008. This amounts to USD 2 928 per person in the Euro zone — equivalent to 7% of average income. According to the Bank for International Settlements, the Euro is the second largest reserve currency and the second most traded currency in the world after the U.S. dollar. The Euro is the official currency of 22 European states with a combined population of approximately 325 million and GDP of EUR 9.8 trillion (USD 13.6 trillion). The Euro has also been adopted as an official currency in Zimbabwe. One Euro equaled USD 1.3917 at December 31, 2008.<sup>9</sup> The highest denomination note is EUR 500 (USD 696). The amount of currency in circulation attributed to the German economy by the ECB grew by nearly USD 100 billion over the period 2003–07. This is demonstrated in Figure 1.

**Figure 1: High denomination banknotes in circulation (in quantities, millions) in the EU**



44. Economic conditions and infrastructure can provide a stable investment environment for money launderers intent on layering and integrating criminal proceeds. In Germany, real growth and real interest rates over the last three years have averaged 2 percent. The Global Competitiveness Report ranks Germany highly for its macroeconomic environment. It is relatively easy to carry out economic activities in Germany: Germany scores 70.5 out of 100 on the Heritage Foundation's Economic Freedom Index and is ranked 25<sup>th</sup> easiest country in the world to do business by the World Bank. Germany's high income levels and large economy also provide plenty of opportunities for large scale ML activity to be carried out unobtrusively.

45. Frankfurt is a major financial center, seat of the European Central Bank (ECB), and a global aviation hub. Thirty-seven of the world's 500 largest stock market listed companies measured by revenue are headquartered in Germany. The 10 biggest are Daimler, Volkswagen, Allianz, Siemens, Deutsche Bank, E.ON, Deutsche Post, Deutsche Telekom, Metro, and BASF.

46. Germany has a large, open, and sophisticated financial system. Total banking sector assets exceed EUR 8.1 trillion (USD 11.3 trillion). Deposits in German financial institutions exceed EUR 3.1 trillion (USD 4.7 trillion). Deposits by non-residents in German financial institutions exceed EUR 1.3 trillion (USD 1.8 trillion). Insurance and financial services provided to non-residents generated

<sup>9</sup> This rate has been used for all currency conversions in this report (except those relating to earlier years) irrespective of whether such conversions would have been better calculated using period averages.

EUR 13 billion (USD 18 billion) in export earnings in 2007. Germany is heavily banked – with approximately 50 bank branches and between 63 and 64 automated teller machines per 100 000 of population. German financial institutions send and receive the third largest volume of SWIFT messages in the world – approximately 616 million annually.

47. The Frankfurt stock exchange is the sixth largest in the world by turnover, with more than EUR 2.4 trillion (USD 3.4 trillion) traded annually. Market capitalization of listed companies exceeds EUR 1.5 trillion (USD 2.1 trillion).<sup>10</sup>

48. German people have access to modern technology with high rates of mobile phone use (118 subscriptions per 100 people), personal computers (66 per 100 people), and internet use (72 users per 100 people).

49. Germany has an open economy and plays a significant role in international trade and investment. Germany scores 2.323 on the Chinn-Ito financial openness variable, which measures a country's degree of capital account openness.<sup>11</sup> The most open economy score is 2.6 and the least open score is -1.8. It is also ranked the 11th easiest country in the world for ease of trading across its borders. Its international trade equates to 86 percent of its GDP. Germany is the world's top exporter. France, the Netherlands, Italy, the United States, and the United Kingdom are Germany's major trading partners. Germany's ports handle the equivalent of nearly 17 million twenty-foot containers annually. Germany is a large investor overseas with a stock of more than EUR 2.4 trillion (USD 3.3 trillion) in portfolio and foreign direct investment. Foreigners have a stock of nearly EUR 3 trillion (USD 4 trillion) invested in Germany, EUR 657 billion (USD 915 billion) in FDI, and some EUR 2.2 trillion (USD 3 trillion) in potentially more volatile portfolio investment.

50. Tourism, workers' remittances, and language also contribute to Germany's international connectedness. Germany was the seventh most popular tourist destination in the world in 2007, with approximately 24 million tourist arrivals. In the same period, more than 70 million tourists departed Germany, the second highest in the world. Outward worker's remittances amount to nearly USD 14 billion annually and approximately USD 8.5 billion are received. The German language is used elsewhere in Europe, namely in Austria, Belgium, the Bolzano province of Italy, Liechtenstein, Luxembourg, and Switzerland, although German speakers are, in some, a small proportion of the population. German is also an official language in Namibia. These other countries have a combined population of 88 million and GDP of EUR 2.7 trillion (USD 3.8 trillion).

51. The contribution of governance issues to ML and TF risks in Germany appears low. Germany is generally regarded as a jurisdiction with strong adherence to the rule of law. It scores well in corruption perceptions indices, despite the existence of some high-profile bribery and corruption cases (*e.g.* Siemens<sup>12</sup> paying USD 1.3 billion in fines in December 2008 after being investigated for serious bribery). Germany scores favorably high scores across the indices in the World Bank World Wide Governance Indicators Country Snapshot:

---

<sup>10</sup> All data for 2007 is from the World Bank's World Development Indicators Database.

<sup>11</sup> More information about this index is available at <http://www.ssc.wisc.edu/~mchinn/research.html>.

<sup>12</sup> AG.

**Statistical Table 2. Germany Governance Indicators**

Indicator	Percentile Rank (0-100)
Voice and Accountability	95
Political Stability/No Violence	81
Government Effectiveness	92
Regulatory Quality	93
Rule of Law	94
Control of Corruption	93
Average	91

52. The CC criminalizes various forms of corruption. Germany signed the United Nations Convention against Corruption (UNCAC) in 2003 and transposed the OECD “Convention on Combating Bribery of Foreign Public Officials in International Business Transactions” into German law in 1998.

53. In addition, the efforts of law enforcement are generally viewed favorably in Germany. Germany scores 6.5 out of 7 in the Global Competitiveness Report’s Reliability of Police Services Index, Germany is perceived as a low security risk by the travel advisory consultancy “ControlRisk”<sup>13</sup>. Germany also has an above average conviction success rate (see Statistical Table 4), suggestive of good police investigative effort. German law enforcement does score middle range in a composite index on police performance based on crime victim surveys<sup>14</sup>.

<sup>13</sup> The lowest rating is “insignificant.”

<sup>14</sup> Van Dijk, Jan. *The world of crime: breaking the silence on problems of security, justice and development across the world*. Los Angeles: Sage Publications, 2008. Van Dijk derives a Composite Police Performance Index: combination of two objective measures (victim reporting rate and homicide conviction rate) and three subjective measures (victim satisfaction, citizen's satisfaction, and business executives' satisfaction), all of which are correlated indicators.

## 1.2. General Situation of Money Laundering and Financing of Terrorism

54. The authorities provided the information in the following table that gives a selection of statistics concerning the AML/CFT regime that operates in Germany:

**Statistical Table 3. Selected Statistics on Germany ML/CFT Regime**

Year	No. of STRs	Value of STRs EUR million	Value of STRs USD million	Provisional Measures Assets Seized		Prosecuted ML Cases	ML Convictions	Property Forfeited & Confiscated EUR million	Property Forfeited & Confiscated USD million
				EUR million	USD million				
2004	8 062	N/A	N/A	N/A	N/A	144	112	305 963 158	425 808 927
2005	8 241	N/A	N/A	N/A	N/A	129	97	319 282 155	444 344 975
2006	10 051	N/A	N/A	N/A	N/A	259	216	300 570 519	418 303 991
2007	9 080	N/A	N/A	N/A	N/A	708	603	218 782 569	304 479 701
2008	7 349	N/A	N/A	N/A	N/A	766	608	N/A	N/A
TOTAL	42 783	N/A	N/A	N/A	N/A	2 006	1 636	1 144 598 368	1 592 937 594

55. Germany is a large internationally connected economy. Its criminal economy can be expected to have similar traits. Germany is classified as a major ML country by the U.S. Government.<sup>15</sup>

56. Statistics issued by the United Nations<sup>16</sup> indicate that Germany records more crimes than the average of the other surveyed countries. They also indicate that Germany has relatively higher incidence of drug-related crimes, burglaries, embezzlements, and frauds. Crimes against the person are proportionally less prevalent. On average, Germany proportionally prosecutes more frequently than other surveyed countries and has less people in prisons.

57. Statistics supplied by the authorities support this analysis. Detailed national crime statistics are compiled by the police and published by the Federal Ministry of the Interior (BMI) annually. The latest available version indicates that 6 284 661 offenses were recorded in Germany in 2007 (77 per 1 000 population) and that the three highest reported crimes were related to: theft (2 561 691 or 31 per 1 000 population), fraud (912 899 or 11 per 1 000 population), and drugs (248 355 or 3 per 1 000 population). The total recorded crimes for 2006 was similar — 6 304 223. The top three single discrete crimes with the highest recorded incidences were shoplifting (408 377), theft of bicycles (372 045), and theft from vehicles (350 034).

<sup>15</sup> International Narcotics Control Strategy Report (INCSR), 2009. Released by the Bureau for International Narcotics and Law Enforcement Affairs, U.S. Department of State, March 2009. A major money laundering country is defined by U.S. statute as one “whose financial institutions engage in currency transactions involving significant amounts of proceeds from international narcotics trafficking.” However, the complex nature of money laundering transactions today makes it difficult in many cases to distinguish the proceeds of narcotics trafficking from the proceeds of other serious crime. Moreover, financial institutions engaging in transactions involving significant amounts of proceeds of other serious crime are vulnerable to narcotics-related money laundering.

<sup>16</sup> Seventh United Nations Survey of Crime Trends and Operations of Criminal Justice Systems, covering the period 1998–2000. Note: Crime statistics are often better indicators of prevalence of law enforcement and willingness to report crime, than actual prevalence of criminal activity.

**Statistical Table 4. Selected Crime Statistics**

Crime Related Statistic	Average of countries surveyed	Germany
Total Crimes	0.75 m	6.3 m
Total Crimes per 1 000 population	34	76
Drug offenses per 100 000 population	191.1	302
Murders per 1 000 population	0.10	0.01
Assaults per 1 000 population	2.5	1.4
Burglaries per 1 000 population	5.1	12.9
Embezzlements and frauds per 1 000 population	1.3	11.1
Police per 1 000 population	3.0	3.0
Adults prosecuted per 1 000 population	10.5	15.0
Clearance Rate (closed cases/reported crimes)		55%
Conviction success rate (convictions/prosecutions)	60%	81%
Prisoners per 100 000 population	148	90

Source: United Nations and BKA.

58. The following cities in Germany recorded more than 100 000 criminal offenses annually in 2007: Berlin (496 163); Hamburg (237 048), Cologne (146 142), Munich (110 677), and Frankfurt (107 078).

59. Germany is a consumer and transit country for narcotics, according to the United States Department of State 2009 International Narcotics Control Strategy Report (INCSR), which is the source for the rest of the information in this paragraph. Germany is not a significant drug cultivation or production country. However, Germany's location at the center of Europe and its well-developed infrastructure make it a major transit hub. The German government actively combats drug-related crimes and focuses on prevention programs and assistance to drug addicts. Cannabis remains the most commonly consumed illicit drug in Germany. Seizures of amphetamines and methamphetamines increased substantially in 2007. Organized crime continues to be heavily engaged in narcotics trafficking. The Federal Criminal Police Office (*Bundeskriminalamt*, BKA) publishes an annual narcotics report on illicit drug-related crimes, including data on seizures, drug flows, and consumption. Ecstasy moves through Germany. Heroin is trafficked to Germany. Cocaine moves through Germany. Germany is a major manufacturer of pharmaceuticals, making it a potential source for precursor chemicals used in the production of illicit narcotics, although current precursor chemical control in Germany is excellent.

60. The authorities publish useful information about estimates of loss, damage, or estimated proceeds or profits from some crimes. The 2007 Situation Report on Economic Crime in the Federal Republic of Germany, published by the BKA, reported total loss or damage from economic crimes only at approximately EUR 4.12 billion (2006: approximately EUR 4.32 billion). The annual criminal statistics contain estimated losses for completed cases in relation to a range of offenses – including offenses that generate proceeds of crime. In addition, the authorities publish a regular report about organized crime. The latest version of that document estimates that the profits of organized crime in Germany amounted to EUR 0.66 billion (USD 0.92 billion) in 2008. This figure seems relatively low compared to the overall proceeds of crime situation and the size of the retail drug market in Germany. The statistics do not address the amount of proceeds generated from evasion of taxes and excise duties. However, the German Finance Minister made a statement to the German parliament on May 7, 2009 to the effect that the government treasury loses about EUR 100 billion (USD 133 billion) in annual revenues due to (legal) tax avoidance and illegal tax evasion (inclusive of tax fraud).

61. Statistical Table 5 shows the results of taking data from various BKA reports and combining them to make estimates of proceeds of crime.

	Recorded Crimes	Estimated Loss or Profit <sup>(b)</sup> (EUR billion)	Other Proceeds or Profit Estimates <sup>(c)</sup> (EUR billion)	Baseline Estimate (EUR billion)	Unreported Crime Adjusted Estimate <sup>(d)</sup> (EUR billion)	Baseline Estimate (USD billion)	Unreported Crime Adjusted Estimate (USD billion)
Robberies and Thefts	2 614 640	3.601		3.601	9.003	5.012	12.529
Fraud Offenses	912 899	2.372	4.00 <sup>(e)</sup>	4.000	10.000	5.567	13.917
Drug Offenses	248 355		8.794 <sup>(f)</sup>	8.794	8.794	12.239	12.239
Human Trafficking			0.037	0.037	0.093	0.052	0.1299
Arms Trafficking			0.005	0.005	0.012	0.006	0.016
Sexual Crimes			0.032	0.032	0.081	0.045	0.113
Counterfeiting and piracy of products			0.029	0.029	0.071	0.040	0.099
Environmental Crime	16 528		0.002	0.002	0.005	0.003	0.007
Insolvency offenses	5 484						
Tax and Excise Evasion			25.00 <sup>(g)</sup>	25.000	25.000	34.793	34.793
Offenses against commercial legislation	7 802	1.609		1.609	4.023	2.239	5.598
Other Crimes			0.021	0.021	0.053	0.030	0.074
<b>Total Crimes</b>	<b>6 284 661</b>	<b>7.583</b>	<b>37.920</b>	<b>43.130</b>	<b>57.135</b>	<b>60.025</b>	<b>79.514</b>
Percentage of GDP		0.2%	1.0%	1.2%	1.6%		
Memorandum Items							
- Money Laundering Offenses	3 923						
- Economic Crimes	87 934		4.200	4.200	10.500		
- Organized Crime			0.663	0.663	1.658		

Notes:

(a) Sources: National crime statistics 2007, Situation Report on Economic Crime in the Federal Republic of Germany, 2007. Narcotic Drugs Annual Report 2007. Organized Crime Situation Report 2008. All published by the BKA.

(b) Takes estimate from BKA crime statistics and apportions it upwards for incomplete investigations.

(c) Unless otherwise noted, these figures are calculated by apportioning estimated profits from organized crime to the crime categories that organized crime was identified as being involved in.

(d) Assumes actual crime is at least 2–3 times reported crime. An analysis of Germany data contained in the UN's 2004–2005 International Crime Victim's Survey and the 2005 European Survey on Crime and Safety provides the following justification for this assumption. The number of victims of profit generating crimes with common titles in the Germany criminal statistics ranged from 2.6 times the recorded level of crime for theft of motor vehicles to 11 times the number of reported crimes for consumer fraud with an average of 7.7. While some of this discrepancy can be explained by some recorded crimes having multiple victims, it lends weight to scaling up the amount of recorded crime by a factor of 2 or 3 to obtain a more realistic picture of actual crime.

(e) Industry estimate of insurance fraud only, conveyed to assessors during on-site mission.

(f) Derived from United Nations Office on Drugs and Crime, 2005 World Drug Report, estimates of the value of retail drug markets.

(g) Based on Finance Minister estimate Bach/Dwenger, "Unternehmensbesteuerung: Trotz hoher Steuersätze nur mäßiges Aufkommen", DIW-Wochenbericht Nr. 5/2007, S. 63 ff.), that total tax avoidance and evasion amounts to EUR 100m per annum. Table assumes 25% is illegal tax and excise evasion.



62. The various sources provide a baseline estimate of around EUR 43 billion (USD 60 billion) for proceeds of crime in Germany inclusive of tax evasion — equivalent to around 1.2% of GDP. Adjusting for unreported crimes results in an upper range of around EUR 57 billion, 1.6% of GDP. The EUR 43 to EUR 57 billion (approximately USD 60 – 80 billion) would appear to be a reasonable bottom of the range estimate given that the shadow economy is estimated at more than EUR 500 billion (USD 696 billion), and, more generally, given the amount of reported crime and the size of the German economy. This is a significant amount of proceeds of crime contributing to the world's ML problem and which potentially need to be laundered — in either Germany or elsewhere. To put it in context, at the end of 2008, there were more than 110 countries each with total GDP that is less than USD 60 billion.

63. The authorities were not able to provide any estimates of the amount of funds being laundered in Germany. They indicated that reliable estimates of any sums and amounts from ML activities are not feasible in Germany and the BKA does not provide such estimates.

64. Germany acknowledges that organized crime operates at a serious level in Germany. Each year, the BKA publishes an Organized Crime Situation Report. The latest available report contains the following summary statistics:

Year	2007	2008
Number of investigations	602	575
Number of suspects	10 356	9 472
Total number of nationalities	113	112
Percentage of German suspects	42.1 %	41.7 %
Percentage of non-German suspects	57.9 %	58.3 %
including:		
Turkish nationals	10.0 %	9.4 %
Polish nationals	4.6 %	5.3 %
Groups operating in more than one area of crime	31.9 %	32.2 %
Estimated profits	EUR 481 m	EUR 663 m
Provisionally seized assets	EUR 38.5 m	EUR 170 m
Seized assets as % of estimated profits		-
International links	85.2 %	87.7 %
Fields of crime		
Drug trafficking and smuggling	37.0 %	38.6 %
Property crime	16.6 %	13.7 %
Crime associated with the business world	15.4 %	16.9 %
Facilitation of illegal immigration	7.0 %	5.6 %
Tax and customs offenses	6.1 %	8.0 %
Crime associated with nightlife	4.7 %	4.9 %
Violent crime	4.2 %	3.8 %
Counterfeiting/forgery	4.7 %	4.3 %
Arms trafficking and smuggling	0.7 %	0.7 %
Environmental crime	0.5 %	0.3 %



<b>Statistical Table 6: Summary Statistics on Organized Crime in Germany</b>		
Investigations including:		
Money laundering	172	186
As percentage of all organized crime investigations	28.6 %	32.3%
Confiscation of assets	175	155
As percentage of all organized crime investigations	29.1 %	27.0%

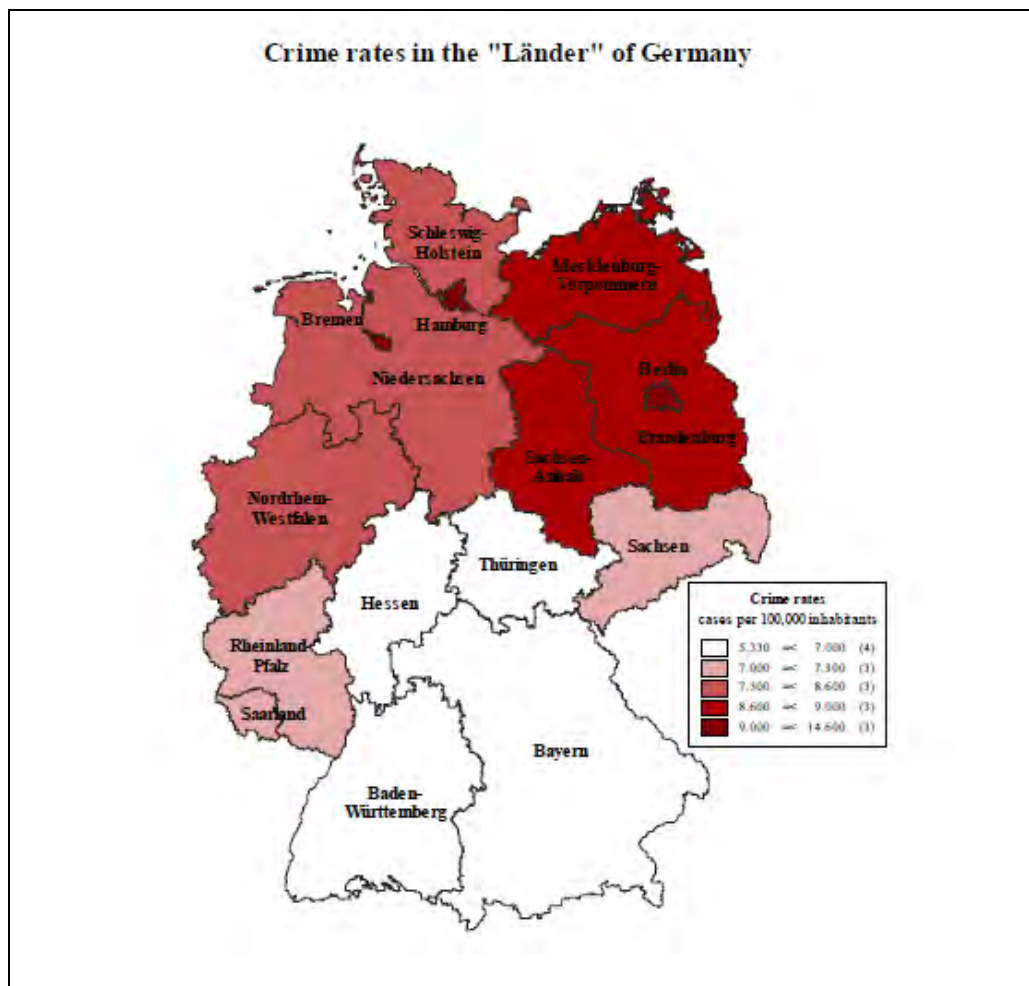
65. The national crime statistics also identify the nationality of offenders. Non-German crime suspects in 2007 totaled 490 278 out of 2 294 883 total suspects (21.4%). The main nationalities were from: Turkey, Poland, Serbia and Montenegro, Italy, and Romania as illustrated in the table following:

**Statistical Table 7: Nationality of Suspects of Crimes, 2007**

<b>Nationality of suspects</b>	<b>Number of Suspects</b>	<b>Percentage</b>
Germany	1 804 605	78.6%
Turkey	108 055	4.7%
Poland	33 291	1.5%
Serbia and Montenegro	30 931	1.3%
Italy	24 607	1.1%
Romania	15 040	0.7%
Russian Federation	13 654	0.6%
Iraq	12 713	0.6%
Greece	9 655	0.4%
Bosnia and Herzegovina	8 910	0.4%
Ukraine	8 479	0.4%
Croatia	8 384	0.4%
Vietnam	8 181	0.4%
France	7 884	0.3%
Lebanon	7 773	0.3%
Morocco	7 470	0.3%
Iran	6 789	0.3%
Austria	6 512	0.3%
The Netherlands	5 758	0.3%
United States	5 610	0.2%
Macedonia	5 536	0.2%
China, PR	5 102	0.2%
Czech Republic	4 734	0.2%
Other	145 210	6.3%
Total Suspects	2 294 883	100.0%
Total Non-German Suspects	490 278	21.4%

66. The domestic distribution of crime suggests that more crime is committed in the north and east of Germany as illustrated in Figure 2:

Figure 2. Crime Rates in the “Länder” of Germany



67. In 2007, 9 080 STRs under the Money Laundering Act were lodged in Germany (2006: 10 051). According to the 2007 Annual Report of the BKA’s Financial Intelligence Unit (FIU), fraud (including computer fraud and investment fraud) were the predicate offenses to ML most frequently recorded by the police (43% of all STRs). Other predicate offenses included, for example, offenses relating to the falsification of documents, tax offenses, breach of fiduciary duty, drug offenses, insolvency offenses, illegal employment, theft and smuggling of illegal immigrants (in that order).

68. The following table shows the total number of prosecutions and convictions over the last four years based on the aforementioned predicate offenses, *i.e.* without any link being established to ML. It is worth noting that the total number of predicate offenses has shown an increasing trend over the four years, whereas the number of STRs received has declined (see also discussion below in relation to R. 13).

Statistical Table 8: Prosecutions and Convictions for main predicate crimes mentioned in STR reports\*

	2004		2005		2006		2007		2008	
	Prose-cutions	Con-victions	Prose-cutions	Con-victions	Prose-cutions	Con-victions	Prose-cutions	Con-victions	Prose-cutions	Con-victions
263-265b of the CC, Fraud	152 891	124 890	172 692	141 518	168 274	137 723	206 995	170 264	199 850	163 987
267-281 of the CC, Document forgery	25 629	21 738	25 693	21 821	23 782	19 959	26 691	22 486	25 068	20 883
Offenses under the Fiscal Code (tax and customs offenses)	13 471	12 055	13 832	12 380	13 004	11 670	17 194	15 573	18 153	16 488
266-266b of the CC, breach of fiduciary duty	12 138	9 826	12 716	10 366	11 668	9 461	12 738	10 383	11 878	9 750
Offenses under the Narcotics Act	57 325	49 739	58 630	51 472	58 892	52 165	64 237	57 116	68 519	61 256
283-283d of the CC, Insolvency offenses	2 062	1 627	2 153	1 712	2 046	1 591	2 055	1 636	1 984	1 570
242-244a of the CC Theft	173 322	142 230	164 641	135 144	154 997	126 070	181 729	147 148	177 550	142 519
Alien smuggling under sections 96 and 97 of the Residence Act	1 889	1 580	1 340	1 117	972	766	1 123	947	1 049	885
Totals	438 727	363 685	451 697	375 530	433 635	359 405	512 762	425 553	504 051	417 364
Convictions as %		83%		83%		83%		83%		83%

\*These data are for all prosecutions or convictions for predicate crimes irrespective of whether an STR is involved. The information for the years 2004 until 2006 represents the situation of the Federal Republic of Germany prior to re-unification, including greater Berlin. The number of convictions and prosecutions for the entire Federal Republic, including the *Länder* of Brandenburg, Mecklenburg-Western Pomerania, Saxony, Saxony-Anhalt and Thuringia, has been recorded only from 2007 onwards.

69. According to the authorities, there is a clear and consolidated culture in German society towards compliance with existing norms in terms of the prevention and repression of ML and TF. They state that ML has often been associated with drug trafficking and drug addiction and that, at present, ML is primarily associated with tax evasion. The authorities also stated that Germany is vulnerable to ML activity because private households prefer to make their payments in cash and the use of cash is high relative to the other countries. The assessors were also told repeatedly that it is common for people who provide services to households (e.g. plumbers) to conduct some of their business in cash outside of the formal economy. The authorities also indicated that they have taken recent steps to address this issue. The authorities also indicated that non-payment of taxes is considered “a sport” by many Germans, and that Germans have an aversion to paying tax on interest income.

70. Most indicators referenced above suggest that Germany may have a higher risk profile for large scale ML than many other countries. It is a large economy and financial center strategically located in the middle of Europe, with strong international linkages. It has a substantial proceeds of crime environment involving organized crime operating in most profit generating criminal spheres. Germany has a large population with a large immigrant component. Germany has open borders and is a significant destination and transit point for international travel. Germany has a large and sophisticated economy and financial sector, plays a large role in world trade, and is involved in large volumes of cross-border trade and financial flows. Germany also has a large informal sector; use of cash is reportedly high. Moreover, the currency of Germany is the Euro which is used widely across Europe, including by organized criminals and tax evaders. The main factors that may help reduce Germany’s risk profile for ML activity are its strong legal tradition, the rule of law, its political environment, Germany’s low levels of corruption, and the consistent approach to prudential regulation and supervision due to the existence of a single Federal level regulator in the financial sector.

### ***Terrorism and Terrorist Financing***

71. Germany considers radical Islamic terrorism as its primary security threat and claims that it has taken extensive domestic measures against such terrorism since September 11, 2001.

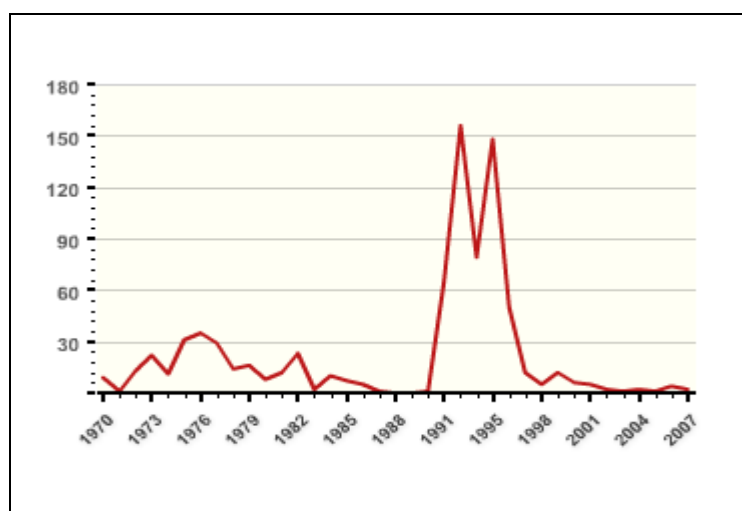
72. Terrorists have carried out terrorist acts on German soil and terrorists have based themselves in Germany prior to carrying out terrorist acts in other nations, including in relation to the September 11, 2001 attacks in the United States. The most recent examples of terrorism in Germany relate to:

- a) An unsuccessful attempt to explode two suitcases filled with bombs on regional trains in Germany on July 31, 2006.
- b) The arrest on November 20, 2006 of six persons being investigated by Federal prosecutors in Karlsruhe for involvement in a foiled plot to smuggle a bomb onto a passenger plane in Germany.<sup>17</sup>
- c) The arrest of three men on September 4, 2007 in the Oberschledorn district of Medebach, Germany who were allegedly attempting to build car bombs.

73. The National Consortium for the Study of Terrorism and Responses to Terror (START), based at the University of Maryland in the United States, Global Terrorism Database<sup>18</sup> contains data about terrorist incidents in Germany since 1970 with the following profile:

---

<sup>17</sup> This investigation is ongoing. At the date that this report was finalized the authorities had not finally concluded whether terrorism charges for this incident could be substantiated.

**Figure 3. Profile of Terrorist Incidents in Germany since 1970**

74. These data suggest that the authorities are experienced in dealing with terrorist related activity. The authorities indicate that a lot of the incidents recorded in this database for the 1990s relates to incidents carried out by groups that Germany does not recognize as terrorist groups. They instead describe these incidents, based on the BKA statistics, as xenophobic criminal offenses committed against asylum seekers and foreigners that may be politically motivated but not terrorist activities.

75. The authorities provided the following official German police statistics of investigations involving initial suspicion of the commission of a criminal offense related to cases of terrorism under Section 129a and 129b of the German CC:

\	2001	2002	2003	2004	2005	2006	2007	2008
Criminal offenses involving terrorism	8	13	42	29	31	49	36	12

Source: BKA.

76. START's Terrorist Organization Profiles (TOPs) database lists 18 terrorist organizations as either operating or that have operated in Germany. The authorities point out that some of the organizations listed in this database are not considered terrorist organizations in Germany and that many others have broken up or their activities curtailed as a result of the German authorities' law enforcement measures. The latter lends support to a view that Germany has a long tradition in dealing (effectively) with terrorist threats, especially home grown terrorism.

77. As of February 2009, the authorities report that 267 criminal investigations relating to Islamist terrorist activities have been conducted in Germany since 2001. Of these, 27 were conducted under section 129a of the StGB and 146 under section 129b of the StGB. The other criminal investigations relate to criminal offenses such as homicide, ML, smuggling of illegal immigrants, violation of foreigners law.

78. The authorities acknowledge that the actual costs for planning and carrying out terrorist activities are quite low, relative to the loss or damage that terrorist attacks can cause. A terrorist group with ample financial resources will, however, be able to achieve its objectives more easily. Thus solvent terrorist groups are more likely to be able to develop the infrastructure (flats, vehicles, communication, forged documents, etc.) necessary to facilitate the commission of a terrorist attack. Findings in Germany show, however, that individual perpetrators or small groups (two to three perpetrators) more or less spontaneously decide without any major logistical effort to plan and carry out terrorist attacks, although in some cases they resort to existing terrorist structures and networks. According to the findings of the Federal and State Security Agencies, both legal and illegal sources and transfer methods are used to finance terrorism.

79. It is highly likely that Germany continues to be exposed to the potential of further terrorist activity and Germany could be expected to have a higher than average risk profile for TF activity.

### 1.3. Overview of the Financial Sector

80. The German financial sector is a motor of the German economy. The banking sector comprises a number of large, internationally active commercial banks as well as a high number of savings and cooperative banks. The insurance market is sizeable. Germany is furthermore home to the sixth largest stock exchange in the world, the Frankfurt Stock Exchange (*Frankfurter Wertpapierbörse*).

81. The German financial system comprises 3 400 institutions approximately. It is dominated by the banking sector. At the end of 2008, out of 2 048 German banking type financial institutions, 1 878 were commercial banks, savings banks, and cooperative banks (universal banks) and 170 other banks. The non-universal banks are specialized in such activities as mortgage banking and investment. In addition, as of September 2009, there were 1 344 financial services institutions (including money transmitter, currency exchange, credit-card, finance-leasing, and factoring businesses).

#### *Banking*

82. Two types of institutions operate in the German banking market: credit institutions, defined as companies involved in “banking business” and financial services institutions<sup>19</sup>. All institutions operating in the German banking market are licensed and supervised by the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin*).

83. The banking sector itself has, in turn, traditionally been characterized as comprising three pillars: commercial banks; savings banks, and the cooperative banking network. The number of banks in each sector is set out in the following table:

	2008	2007
Commercial banks	183	204
Savings banks	448	458
Credit cooperatives	1 247	1 281
Other institutions	170	131
<b>Total</b>	<b>2 048</b>	<b>2 074</b>

<sup>19</sup> December 31, 2008: 1 347 financial service institutions (the exact number of leasing and factoring companies is not yet clear).

84. The commercial bank sub-sector, which holds less than 30% of system-wide assets, is relatively concentrated due to the size of the four largest, internationally active banks. This sub-sector also includes a number of subsidiaries of foreign banks.

85. The savings banks (*Sparkassen*) are retail banks that are normally market leaders in their respective localities. The majority of them are owned by administrative districts and municipalities. The State Banks (“*Landesbanken*”) are mainly owned by the States and the savings banks. The credit cooperatives (credit unions — “*Volksbanken*” and “*Raiffeisenbanken*”) are owned by their members. All types of bank groups are headed by apex or regional associations which provide marketing and common services support to all their member banks.

### ***Insurance***

86. With premium income in 2007 of EUR 163 billion (USD 227 billion), Germany is the fifth largest insurance market in the world after the U.S., Japan, the United Kingdom, and France. With total assets under management of EUR 1.3 trillion (USD 1.8 trillion), the German insurance industry fulfils its function as a financial intermediary for term coverage and provisions for retirement income and surviving dependents. With approximately EUR 700 billion (USD 974 billion) on their balance sheets in total, the AML-relevant life insurance companies and accident insurance companies with premium redemption are a major factor in the German financial market.

87. Insurance companies in Germany are restricted in terms of the risks they can insure — a life insurance company cannot also sell health insurance, and *vice versa*. However, it is possible (and common) for parent companies to hold subsidiaries in each of the areas of insurance.

88. Federal insurance companies are licensed and supervised by the BaFin. Insurance companies operating only in a single *Land* are regulated by the respective *Länder* authority.

### ***Securities Industry***

89. The Frankfurt Stock Exchange is one of the world’s largest trading centers for securities. The most stock trading is conducted via the Frankfurt Stock Exchange and Xetra (as of March 2008, they accounted for 98% of trading in German shares and 84 percent in foreign shares). Deutsche Börse AG operates the Frankfurt Stock Exchange, an entity under public law. The Frankfurt Stock Exchange facilitates advanced electronic trading, settlement and information systems. Today, the Frankfurt Stock Exchange is an international trading centre. This is also reflected in the structure of its participants. Some 160 of around 330 market participants come from abroad.

90. There are six other regional stock exchanges based in: Stuttgart, Munich, Hamburg, Düsseldorf, Hannover, and Berlin. In addition, the derivatives exchange Eurex is based in Frankfurt, the European Energy Exchange in Leipzig, and the Risk Management Exchange in Hanover.

91. The proper conduct of exchange trading, as well as the correct pricing process, is monitored by the Trading Surveillance Office (*Handelsüberwachungsstelle*). The exchange supervisory authorities (*Börsenaufsichtsbehörden*) are responsible at the *Länder* level.

92. According to German law, all business related to securities trading is considered either banking business or financial services and as such are subject to a licensing requirement. This ensures that the entire securities sector is regulated and supervised. In the field of asset management, the BaFin regulates and supervises credit institutions and financial services institutions on the basis of the Banking Act and capital investment companies, custodian banks, investment funds, and investment stock corporations on the basis of the Investment Act (*Investmentgesetz, InvG*).



93. In the investment services sector, all financial intermediaries fall under German legislation. Natural persons, as well as enterprises providing investment services on a professional basis by mediating transactions relating to financial instruments between retail clients, other intermediaries or professional clients or execution venues such as regulated markets or other trading platforms, require authorization granted by the BaFin. However, there are some exemptions for persons providing certain investment services only as an ancillary service to another main business activity outside the capital markets.

94. The following statistical table sets out the types of financial institutions that can engage in the financial activities that are within the definition of “financial institutions” in the FATF 40+9 (data as of end of 2007<sup>20</sup>):

**Statistical Table 9. Financial Activity by Type of Financial Institution**

Type of financial activity	Type of financial institution that performs this activity	No. of institutions (a)	Combined balance sheet (EUR billion)	Average balance sheet (EUR billion)	Combined balance sheet (USD billion)	Average balance sheet (USD billion)	Supervisor
1. Acceptance of deposits and other repayable funds from the public (including private banking)	Deposit-taking German credit institutions are “ <b>universal banks</b> ”, and are also licensed for all other banking business	1 878	8 390.0	4.468	11 676.4	6.217	BaFin
2. Lending	Active institutions hold licenses for lending and deposit-taking	1 878	8 390.0	4.468	11 676.4	6.217	BaFin
3. Financial leasing	<b>Financial leasing companies</b> (b)	600 (est.)	N/A	N/A	N/A	N/A	BaFin
4. The transfer of money or value (including financial activity in both the formal or informal sector)	Universal banks are licensed money transmitters.	1 878	8 390.0	4.468	11 676.4	6.217	BaFin
	There are licensed <b>money remittance agencies</b> (c)	38	15.5	0.408	21.6	0.568	BaFin
5. Issuing and managing means of payment	See number 1 above.	1 878	8 390.0	4.468	11 676.4	6.217	BaFin
	In addition, there are <b>credit card companies</b> and	4	1.2	0.300	1.7	0.418	BaFin
	<b>e-money institutions</b>	9	0.04	0.005	0.1	0.007	BaFin
6. Financial	See number 1						

<sup>20</sup> For purposes of this overview, the numbers listed correspond to the end of 2007, the last date for which complete balance sheet data is available. In the remainder of the MEQ, the numbers of institutions listed reflect the number on the day it was written.



Type of financial activity	Type of financial institution that performs this activity	No. of institutions(a)	Combined balance sheet (EUR billion)	Average balance sheet (EUR billion)	Combined balance sheet (USD billion)	Average balance sheet (USD billion)	Supervisor
guarantees and commitments	above.	1 878	8 390.0	4.468	11 676.4	6.217	BaFin
	There are also <b>guarantee business</b> not licensed for deposit-taking	20	1.3	0.067	1.9	0.093	BaFin
7. Trading in: (a) money market instruments; (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading	See number 1 above.	1 878	8 390.0	4.468	11 676.4	6.217	BaFin
	There are also <b>securities trading banks</b> , not licensed for deposit-taking	39	2.1	0.054	2.9	0.075	BaFin
8. Participation in securities issues and the provision of financial services related to such issues	See number 7 above.	1 878	8 390.0	4.468	11 676.4	6.217	BaFin
		39	2.1	0.054	2.9	0.075	BaFin
9. Individual and collective portfolio management	Financial services institutions licensed for <b>individual portfolio management</b> ) as well as <i>Kapitalanlagegesellschaften</i> ( <b>capital investment companies</b> ) and <i>Investmentaktiengesellschaften</i> ( <b>investment stock companies</b> ) according to Section 2 (5) and (6) of the Investment Act.	455	1.3	0.003	1.8	0.004	BaFin
		74	0.6	0.008	0.8	0.011	BaFin
10. Safekeeping and administration of cash or liquid securities on behalf of other persons	See number 1 above. In addition, there are credit institutions not licensed for deposit-taking that are licensed according to Section 1 (1) number 5 of the Banking Act	1 878	8 390.0	4.468	11 676.4	6.217	BaFin
		27	N/A	N/A	N/A	N/A	BaFin

Type of financial activity	Type of financial institution that performs this activity	No. of institutions(a)	Combined balance sheet (EUR billion)	Average balance sheet (EUR billion)	Combined balance sheet (USD billion)	Average balance sheet (USD billion)	Supervisor
	(safe custody business)(d). <sup>21</sup>						
11. Otherwise investing, administering or managing funds or money on behalf of other persons	See number 1 above. In addition, there are <b>capital investment companies</b> and <b>investment stock companies</b> according to Section 2 (5) and (6) of the Investment Act.	1 878	8 390.0	4.468	11 676.4	6.217	BaFin
		74	0.6	0.008	0.8	0.011	BaFin
12. Underwriting and placement of life insurance and other investment related insurance (including insurance undertakings and insurance intermediaries (agents and brokers))(e)	Insurance companies offering <b>life insurance</b> (section 11 et seq. of the Insurance Supervision Act).	103	778.5	7.558	1 083.4	10,519	BaFin
	Insurance companies offering <b>accident insurance with premium redemption</b>	39	105.1	2.695	146.3	3.750	BaFin
13. Money and currency changing	See number 1 above. In addition, there are financial services institutions, licensed for <b>currency exchange only</b> .	1 878	8 390.0	4.468	11 676.4	6.217	BaFin
		22	0.04	0.002	0.05	0.002	BaFin
Total		3 308	9 295.7	2.810	12 936.8	3.911	

(a) Balance sheet sums do not include institutions exempted from supervision until 25 December 2008 according to Section 2 of the previous AML Act.

(b) No statistical data, as these companies only came under supervision on 25 December 2008.

(c) 39 domestic branches registered. However, Deutsche Postbank AG, for example, serves as intermediary for Western Union.

(d) No mandatory reporting.

(e) Data exclude insurance intermediaries supervised by the Länder.

95. The authorities provided the following information about the international dimensions of the German financial system:

<sup>21</sup> This does not include businesses operating in the armoured car industry. They are involved in safekeeping and administration of cash on behalf of other persons, and as such, are defined as a financial institution under the FATF 40+9. This industry's lack of inclusion in the Germany AML regime is not considered a major issue, including due to the fact that the industry is often overlooked in assessment reports.

**Statistical Table 10. Foreign Financial Institutions, 2008**

	Number of branches abroad	Number of subsidiaries abroad
German financial institutions	331	N/A
	Branches and subsidiaries operating in Germany	Supervisor
Foreign banks	192 <sup>22</sup>	BaFin

#### 1.4. Overview of the DNFBP Sector

96. The DNFBPs that are subject to AML/CFT obligations encompass a wide range of businesses and professions. In some cases, the scope of coverage in Germany is broader than that called for in the FATF recommendations. The scope includes businesses, liberal professions (self-employed professionals), and others.

97. The professions, which are all subject to specific legislation regulating their activities, include lawyers, who total approximately 150 000, regulated under 28 separate regional chambers of lawyers. Patent attorneys number approximately 2 800, organized under a single nationwide Chamber of Patent Attorneys. Notaries, who play a central function in verifying the legal provisions of real estate and corporate transfer contracts, number approximately 8 400 persons, organized into 21 regional Chambers of Notaries, each under the oversight of regional courts. An additional category of legal professionals, registered legal advisers, is provided for in the Legal Services Act in 2007. The professionals in this category (which was also provided for in the predecessor 1935 Legal Consultancy Act) provide specialized legal advice with respect to debt collection, pensions, and foreign law. Approximately 3 800 legal advisers are registered nationwide.

98. In the accounting professions, there are approximately 14 000 qualified auditors, organized under a single national Chamber of Auditors. A distinction is usually made between auditors and chartered accountants, with only auditors being qualified to certify the final annual accounts of listed companies and other public interest companies, as defined in Section 319 of the German Commercial Code. Chartered accountants are authorized to carry out and certify the statutory audits of final accounts of smaller and unlisted companies. Chartered accountants are now subsumed under the general auditor profession. The business of accounting firms typically consists of about one-third assurance services (auditing), one-third tax services, and one-third consultancy. About two-thirds of auditors are cross-qualified as either lawyers or tax advisors. Auditors may maintain auditors' trust accounts at banks. These arise particularly in insolvency practices, but also as part of their consultancy services, auditors may manage and administer financial accounts for some clients, usually foundations or wealthy clients. This activity, however, is more typically handled by banks.

<sup>22</sup>

118 branches (9 from non-EEA jurisdictions) and 74 subsidiaries (18 from EU or EA jurisdictions).

99. Tax advisors, who can compile end-of-year statements and prepare tax returns but may not carry out statutory audits, are recognized and regulated as a distinct part of the accounting profession under the Tax Consulting Act. Tax advisers are typically organized as 2–3 person offices or as large tax consulting firms. For the small firms, typical clients are small- and middle-sized firms. Tax advisers are subject to the same AML/CFT obligations as auditors. They number approximately 85 000 persons and are organized into 21 regional chambers.

100. In addition to these liberal professions, the DNFBP sector includes the unregulated real estate agents business, which numbers approximately 12 000. No national statistics were available for the scale and scope of business conducted by real estate agents. Under the AML Act, all persons who deal in goods are subject to AML/CFT obligations. This category includes the DNFBP sectors of dealers in precious metals and dealers in precious stones. According to the Federation of German Jewellery, Watches, Clocks, Silverware and Related Industries, in 2008 there were approximately 390 firms with more than 49 employees engaged in the wholesale jewelry and silverware products industry, excluding retail trade. Total employment is estimated at 6 140. Annual domestic turnover amounted to EUR 807 million (USD 1 123 billion), with exports of EUR 884 million (USD 1 230 billion) and imports of EUR 774 million (USD 1 077). Gold and platinum jewelry accounted for 76% of turnover and silver jewelry accounted for another 10 percent of turnover.

101. Casinos are subject to AML/CFT obligations. There are approximately 80 casino locations in Germany, 49 of which offer table games and slot machines and another 31 which operate slot machines only. A total of 19 companies operate casinos under a mix of private and public ownership. Eleven purely private companies account for 40% of turnover and eight companies in public ownership (mainly or totally) account for 60% of turnover. Casinos operate in 14 of the German federal states, subject to specific legislation in each of the *Länder*. Casino activity has been in decline in recent years, in part because of legislative initiatives to curb problems related to addictive gambling. No national statistics are available on casino activity.

102. Trust and Company Service Providers (TCSPs), to the extent they are not separately covered as lawyers, notaries, independent legal professionals, or accountants, are subject to the AML Act. The broad range of trust and company services identified in the Glossary to the Methodology is not typically organized as a separate line of business in Germany so the country does not have a well-developed, distinct TCSP sector. Rather, such services are primarily provided by lawyers, independent legal professionals, notaries, or accountants. However, there are independent German companies, not run by a covered profession, that do provide office services such as accommodation mailing addresses, mail handling, and telephone answering services. While these office services companies are subject to AML/CFT obligations, no regulatory arrangements have been developed to ensure compliance and no statistics were available on the scale and scope of business handled by independent office service companies.

Statistical Table 11. Structure of DNFBP Sector, 2008

	Number	Authorized/ Registered or Supervised by:	AML supervisor
Legal Profession			
Lawyers	150 000	28 regional chambers of lawyers	28 Regional Chambers of Lawyers
Patent lawyers	2 800	National chamber of Patent attorneys	National Chamber of Patent attorneys
Notaries	8 400	21 regional chambers of notaries	116 Regional Courts
Registered legal advisers	1-2 000	21 Regional Courts	21 Regional Courts
Accounting professions			
Qualified auditors and chartered accountants	14 000	National Chamber of Auditors	National Chamber of Auditors
tax advisors	85 000	21 regional chambers of tax advisors.	21 regional Chambers of Tax Advisors
Other:			
Real estate agents	12 000	unregulated	16 <i>Länder</i> Governments
Dealers in precious metals and stones	390 wholesalers	unregulated	16 <i>Länder</i> Governments
Casinos	80 approx	14 <i>Länder</i>	14 <i>Länder</i> Governments
Trust or Company Service Providers	Unknown	16 <i>Länder</i> Governments	16 <i>Länder</i> Governments

### 1.5. Overview of commercial laws and mechanisms governing legal persons and arrangements

103. Several types of legal entities may be established under German law, mainly under its company law which differentiates between corporations (*Körperschaften*) and partnerships (*Personengesellschaften*).

104. **Corporations** are legal entities separate and distinct from their associates or shareholders. There are five types of corporations under German law:

- The Limited Liability Company (*Gesellschaft mit beschränkter Haftung*, GmbH);
- The Stock Corporation (*Aktiengesellschaft*);
- The Cooperative (*Genossenschaft*);
- The Registered Association (*eingetragener Verein*); and
- The Foundation (*Stiftung*), in some instances.

105. All have legal capacity. They can therefore own assets, are subject to rights and obligations and are capable of being a party to legal proceedings. The most frequently used corporations in Germany are the Limited Liability Companies (of which there are about 980 000) and the Stock Corporations (of which there are approximately 17 000).

106. **Partnerships** take the form of the association (*Verein*). They may be defined as a group of persons who contractually agree to promote a shared objective. Unlike corporations, not all partnerships have legal capacity. According to prevailing opinion in legal literature, even partnerships that have legal capacity are not legal persons *per se*. An association that has no legal capacity is not a partnership either. It is true that in providing for associations without legal capacity, Section 54 of the Civil Code (*Bürgerliches Gesetzbuch*) makes a reference to the stipulations governing corporations; however, this reference is outdated and the adjudication handed down by the courts as well as the legal scientific literature generally acknowledge that sections 21 *et seq.* of the Civil Code, regarding the registered association, are to be applied to associations not having legal capacity as well.

107. Legal arrangements may also be concluded in the form of the *Treuhand*. Not every German *Treuhand* is regulated by law; it is mainly the result of case law and doctrine. It is a very flexible arrangement by which the *Treugeber* places assets under the control of the *Treuhänder* for a specific purpose. In some instances, it is very similar to the Anglo-Saxon trust. While some forms of *Treuhand*s must be disclosed to be effective towards third parties, others remain private.

108. The typical Anglo-Saxon trust may not be established under German law. The authorities were not aware of foreign trusts being administered from Germany and the German government did not ratify The Hague Convention on the recognition of foreign trusts.

## 1.6. Overview of strategy to prevent money laundering and terrorist financing

### *AML/CFT Strategies and Priorities*

109. The main policies and objectives of the German government for combating ML or TF relate to coming into compliance with international obligations to implement an effective AML/CFT regime. Hence, the current focus lies in monitoring the proper implementation of the Third EU Money Laundering Directive (Directive 2005/60/EC of October 26, 2005), and, through that implementation, improving Germany's compliance with the FATF 40+9 Recommendations. The practical current focus of this objective relates to implementing the Act Supplementing the Act to Fight Money Laundering and Terrorist Financing (*Geldwäschebekämpfungsergänzungsgesetz*, GwBekErG), which came into force on August 21, 2008, by educating affected parties about its contents, answering questions, and solving implementation problems that arise.

110. Specifically, in relation to combating TF, Germany's strategy is anchored in a comprehensive counter-terrorism strategy comprising four dimensions, of which the following two are especially significant for fighting TF:

- a. **Operational approach (threat prevention and prosecution):** This approach includes structural investigation to establish and substantiate suspicion, in which financial investigations represent an important element for establishing structural connections, both in order to identify perpetrators and prevent planned activity, and to stop the flow of funding and freeze or seize financial assets. Key factors for success include:
  - i. Early and proactive information-gathering (*e.g.* intelligence services having the right to information in advance of any specific threat or initial suspicion as defined in the CC).
  - ii. Close information-sharing networks (in particular through the Joint Counter-Terrorism Centre (GTAZ), in which all competent security authorities cooperate, and the counter-terrorism database, which contains all the counter-terrorism information gathered in Germany).
  - iii. Pooling of resources or the efficient division of labor (for example in the Joint Internet Surveillance Centre, where the federal security authorities share the task of monitoring the Internet).
  - iv. A comprehensive response, for example, including association bans and seizing assets of organizations. Further, the EU regulations on combating the financing of Al Qaeda and the Taliban (implementation of the UN lists under Community law) also apply in Germany.

111. The authorities state that this operational approach has proved very successful, resulting in a number of convictions on charges of TF and in association bans: Al-Aqsa e.V., which collected donations for Hamas, was banned and its assets confiscated in 2002 on the basis of intelligence service investigations using bank information, and Yatim-Kinderhilfe e.V., which intended to continue the work of collecting funds for Hamas, was banned and its assets confiscated in 2005.

- a. **Protection:** This mainly entails preventing opportunities for crime to take place, including steps taken by the financial sector to prevent TF, such as:
  - i. Providing for possible future investigations (in particular, by means of identification, documentation and retention requirements).
  - ii. Establishing and reporting suspicious activity, also via the internal organization of the financial sector and its reinforcement with government support (*e.g.* typologies).

112. Such action is largely based on the relevant FATF standards, including best-practice recommendations. The authorities state that, given the complexity of TF, this approach has not been as effective, especially with regard to the financial sector itself generating useful reports of suspicious activity, as the operational approach described above, which is one priority of the strategy for combating TF. Further, Germany believes that most sources of funding for Islamist terrorism lie outside Germany's area of sovereignty.



113. A key part of the overall strategy involves analyzing the implications of FIU identified ML and TF typologies and FATF typologies or other findings for Germany and to modify or adopt adequate measures.

114. The authorities also indicate that the fight against ML in Germany is based largely on preventing anonymous money flows and opaque conveyance of title under property law. By largely preventing the undetected introduction of incriminated funds into legal circulation, offenders are denied the ability to secure their proceeds of crime. The authorities contend that this not only serves to combat ML, but also generally reduces the incentive to commit offenses.

115. The authorities also state that a current priority is to use the AML/CFT regime to fight against tax evasion, as the authorities have identified that, at present, ML is significantly associated with tax evasion

116. The Money Laundering Contact Group<sup>23</sup> is also focusing on developing adequate countermeasures in relation to the following three groups that it has identified as being of particular interest:

- a) Professional fields and areas of business in the German economy,
- b) Products, and
- c) Societal actors and professions.

### ***The Institutional Framework for Combating Money Laundering and Terrorist Financing***

117. The key government and nongovernment Ministries, regulatory and other authorities, and other bodies involved in combating ML or TF are set out below.

118. Policy Ministries:

- a) **The Money Laundering Contact Group (MLCG)** is an informal coordinating body on AML/CFT matters comprising representatives of the Federal Ministry of the Interior (Bundesministerium des Innern, BMI), the Federal Ministry of Finance (Bundesministerium der Finanzen, BMF), the Federal Ministry of Justice (Bundesministerium der Justiz, BMJ) and the Federal Ministry of Economics (Bundesministerium für Wirtschaft, BMWi). The latter, while a member, is not an active participant. The group was established in 1993. On a regular basis, also delegates from the BaFin, from the *Bundesbank*, and from the FIU (and if required also from other concerned authorities or from the private sector) participate in the meetings of the MLCG.
- b) **The Federal Ministry of Finance (BMF):** is responsible for the legislation in the field of banking, insurance, brokering, and securities business as well as for customs and fiscal matters. This responsibility includes the legislation on preventive measures against ML and TF in the financial sector. The BMF has the leading role for legislative procedures concerning directives and regulations of the European Community dealing with financial issues as well as with AML/CFT. The BMF exercises legal and supervisory control over The BaFin, the Customs Criminological Office and the customs offices in the field of countering ML and TF among others.

---

<sup>23</sup> See next Section for more information about this group.



- c) **The Federal Ministry of Justice (BMJ):** Responsible for legislation pertaining to substantive criminal law and the law on criminal procedure. The BMJ, in conjunction with the Federal Foreign Office and other affected ministries handles and makes mutual legal assistance (MLA) requests, unless responsibility for the provision of legal assistance rests with an authority belonging to the portfolio of a different federal ministry, in which case the decision would then rest with such ministry. The power concerning requests to and from specific countries and relating to specific forms of MLA has been delegated to the *Länder* governments — and the enforcement authority for legal assistance requests is always the locally responsible public prosecutor with the Regional Court. The Federal Attorney General (Generalbundesanwalt), who is under the purview of the BMJ, takes action in cases of criminal offenses with a terrorist background (sections 129a and 129b of the CC). The BMJ is also responsible for the law relating to legal persons and arrangements.
- d) **The Federal Ministry of the Interior (BMI)** has a wide spectrum of tasks ranging from internal security, policy in the field of asylum and foreigners, the public service, modernization of the administration and constitutional law to sport. Focal tasks of the BMI in the field of internal security include combating ML and TF, in particular:
1. Development and adoption of measures, including legislative measures, to deter ML and TF. Therefore, it has the main task to review the effectiveness of the system to combat ML and TF schemes by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency.
  2. Implementation of the provisions issued by the EU.
  3. Implementation of the FATF Recommendations.
  4. Expert supervision of the BKA sections responsible for combating ML and TF, which includes Germany's Financial Intelligence Unit (FIU).
- e) **The Federal Ministry of Foreign Affairs (AA)** through the Federal Foreign Office is responsible for international cooperation in the fight against terrorism and organized crime, including international cooperation against ML.
- f) **The Federal Ministry of Economics and Technology (BMW)** is responsible for the Foreign Trade and Payments Act (*Außenwirtschaftsgesetz* - FTPA) and, in conjunction with *Deutsche Bundesbank* and the Federal Office of Economics and Export Control (BAFA), for the implementation of financial sanctions regarding the fight against the financing of terrorism. *Deutsche Bundesbank* is in charge of the administrative implementation of the freezing of funds. The Federal Office of Economics and Export Control (BAFA) is responsible for the administrative implementation of freezing orders on economic resources and other assets.

119. Criminal justice and operational agencies:

- a) **The Federal Criminal Police Office (BKA)** is Germany's central police agency. It is an essential cornerstone in a comprehensive system of crime control and works as a partner with the police forces of the Federation and of the individual German states. According to the German Constitution, for the most part police jurisdiction in Germany lies with the 16 German states. To co-ordinate crime suppression at national and international level, the BKA

was established as the central office for police information and communications as well as for the German CID. By acting as information and communications centre of the German police, the BKA provides support to the police forces of the federation and of the states in connection with the prevention and prosecution of crimes that involve more than one German state and that are of international significance or otherwise of considerable significance. A number of centralized systems and facilities for the German police are maintained at the BKA. This is where the most important police messages come together, and this is also where information about criminal offenses and criminals is stored in a central location. New crime suppression methods are investigated and developed here to ensure that the police are always state-of-the-art in terms of science and technology. The BKA has also been assigned the task of promoting police co-operation in Europe and throughout the world as a legal mandate. All official communications between the German police and other countries are routed through the BKA. The BKA acts as the national central office for Interpol, Europol and the Schengen Information System.

- b) **Financial Intelligence Unit (FIU)** is a special subsection within the BKA. The FIU is also responsible for international information-sharing with other FIUs.
- c) **Public prosecutor's offices** within each *Länder* pursue cases for ML offenses that occur within that *Länder's* jurisdiction. They also generally have special departments, which deal with the implementation of measures to recover or confiscate assets.
- d) **State Bureaus of Criminal Investigation (LKA)** within each *Land* are responsible for crime control within that *Land's* jurisdiction. Each LKA includes financial investigation officers who are subject to direction by the public prosecutor's officers when investigating ML and TF offenses.
- e) **Asset Recovery Offices (AROs):** On the basis of EU Council Decision 2007/845/JHA Germany appointed two authorities as AROs to support the cross-border exchange of information for detecting and identifying assets. The tasks of the German AROs are performed by the Federal Office of Justice (Bundesamt für Justiz) from the judicial side and by the BKA from the police side.
- f) **The Federal Customs Administration** is the national border control agency and it has the task of monitoring cross-border cash movements.
- g) **The Customs Investigation Service (ZFD)** is the investigation service of the federal customs administration. It is organized nationally and does not fall under the jurisdiction of the individual *Länder*. Customs investigation officers are investigating officers of the public prosecutor's office and have the same rights and duties as police officers. The customs investigation offices (*Zollfahndungsämter*) and the **Customs Criminal Office (Zollkriminalamt [ZKA])** are generally the competent criminal prosecution offices within the meaning of Section 11 (1) of the Money Laundering Act. This implies that they may also receive reports of suspected cases from those institutions obliged to submit such reports under the Money Laundering Act. Pursuant to Section 1 (3c) of the Customs Administration Act (CAA), the customs investigation offices have the task of investigating and prosecuting internationally-organized ML and related criminal offenses to the extent that these are connected to the movement of goods from and to external territories. Investigations conducted by the Customs Investigation Service into ML activities are carried out by order of the respective competent state prosecutors (who, under the Courts Constitution Act, have the authority to instruct all investigators), who are duly notified of the investigation results and

then decide how to proceed (for example, whether to discontinue investigations or bring a charge).

120. Financial sector bodies:

- a) **The Federal Financial Supervisory Authority (BaFin)** is Germany's integrated financial supervisory authority responsible for regulation and supervision of the entire financial system. Its tasks include preventing any abuse of the financial system for the purposes of ML and TF. These responsibilities are carried out in the Money Laundering Prevention Group (MLPG).
- b) **The Central Bank (*Deutsche Bundesbank*)** plays a major role in banking supervision in cooperation with The BaFin. The *Bundesbank* does not possess any sovereign powers in combating ML, but it is involved in coordination efforts to combat ML both nationally and internationally. At the national level, the *Bundesbank* participates in all legislative measures in an advisory capacity. It is represented in the Money Laundering Contact Group by the Federal Ministry of Finance. At the international level, a representative of the *Bundesbank* is a member of the German delegation at the meetings of the FATF. The *Bundesbank* administers the restrictive measures imposed through financial sanctions and is the competent authority regarding funds. It collects information and may issue authorizations for exemptions.

121. DNFBP and other matters

- a) **Casino supervision body.** There is no national casino regulator. Instead, casinos are regulated at the *Länder* level usually by the interior ministry.
- b) **Professions:** AML/CFT oversight of the regulated professions is conducted by the authorities and institutions of each *Länder* or by SROs. The SROs are professional bodies, organized under public and, in this context, mostly national law, and are responsible for self-regulation of the profession within their jurisdiction. Examples of SRO include the following:
  1. Bar associations
  2. Chambers of tax advisers
  3. Chamber of public accountants
  4. Chambers of patent attorneys

The chambers of notaries are professional associations but, since notaries are holders of public office, the chambers do not have SRO functions. Rather, notaries are supervised by presidents of regional courts.

- c) **Other DNFBPs:** The real estate agents, dealers in precious metals and dealers in precious stones come under trade law. Because of the way competencies are divided in the Basic Law, this means that the *Länder* are responsible for these groups. The 16 *Länder* have introduced various different arrangements for the supervision of these two professional groups. In some *Länder*, the interior ministry is responsible.

122. Registry for companies and other legal persons, and for legal arrangements:

- a) **The commercial register (*Handelsregister*)** in Germany is a public register holding entries about the registered merchants (*Kaufleute*) including information (such as on the founders, boards) of all commercial companies, and is held by the district of the competent register court (*Registergericht*). The commercial register is maintained by the local courts as the register courts.

In most cases, the local jurisdiction falls to the local court in whose district the relevant regional court is located. A judge or registrar is responsible for making entries in the register. An electronic form of the commercial register has been in place in Germany since 2007. The commercial register is for publicizing information, providing evidence and acting as a control mechanism and protective measure. Anyone may request a print-out or can inspect the corresponding files without having to substantiate the request.

- b) **The register of cooperatives** (*Genossenschaftsregister*) in Germany is a public register providing information about the legal status of a registered cooperative (*eingetragene Genossenschaft, eG*). Anyone may request a print-out or can inspect the corresponding files without having to substantiate the request.
- c) **The register of associations** (*Vereinsregister*) is a public register holding entries about registered associations. Associations are established pursuant to the provisions of the Civil Code (which is where the law on associations is set out). The register is maintained at the local courts (with subject-matter jurisdiction). Entry into the register of associations is possible upon application. Through entry in the register, the association becomes a registered association (*eingetragener Verein*) and its name carries the corresponding abbreviation “e. V.”

123. Non-profit organizations

- a) All non-profit associations established pursuant to the provisions of the Civil Code are registered in the register of associations if they apply for this to be done. There is no specific mechanism in Germany for the supervision of NPOs.

***Approach Concerning Risk***

124. The authorities informed the assessors that there has been no national assessment undertaken of the ML risks in Germany. They advised that the federal security authorities (BKA, Federal Office for the Protection of the Constitution (BfV) and the Federal Intelligence Service (BND)) regularly produce joint situation reports on TF which include a risk assessment. The assessors were not provided with a copy of that assessment due to its sensitive nature.

125. While there may not have been a formal national ML risk assessment undertaken, the authorities claim, that they regularly assess the existing system relating to the prevention of ML and TF in Germany through the following mechanisms:

- a) The FIU publishes an annual report providing an overview of the suspicious operations notified as well as an indication of the financial entities, non-financial businesses and professions that are most active on this issue.
- b) The BaFin publishes an annual report which gives an overview of its activities and important events and developments during the reporting period. This also includes a chapter on the activities of the BaFin’s MLPG and the essential findings resulting from its AML-supervisory tasks with regard to banks, insurance undertakings, financial services institutions, investment stock corporations and capital investment companies.
- c) The BaFin holds meetings regularly with the industry associations in which practical issues in implementing and interpretation of the legal AML/CFT-requirements as well as the effectiveness of practical procedures and supervisory requirements are subject to discussions.

- d) There are periodical meetings between the authorities (in particular the FIU) and financial and non-financial bodies (*Verbände und Kammervvertretungen*) to discuss the potential difficulties in applying existing legal provisions. These meetings have led to improvements in procedures, such as the feedback for entities which notify the authorities of suspicious or unusual operations. Furthermore, representatives of the BaFin do regularly take part in seminars of the financial services industry on AML/CFT issues and illustrate the administrative practice of the BaFin on the implementation of the AML/CFT framework.
- e) There are regular meetings of all Ministries and authorities involved in the German FATF delegation. These Ministries and authorities are also part of the so-called AML/CFT-Contact Group, which holds its meeting regularly in order to discuss apart from question relating to the implementation of international standards.
- f) Once a year, the German Government surveys the federal authorities about the implementation of Government measures relevant to combating terrorism (including measures and projects to combat TF).

126. Germany has adopted a risk-based approach (RBA) in the AML Act, Banking Act and Insurance Supervisory Act. The RBA replaced the previous “rule-based approach.” The RBA applies to the obligations of institutions, particularly due diligence obligations, and also governs the BaFin’s approach to supervision. The RBA is aimed at enabling measures to combat ML and TF to be structured in a more targeted and more efficient manner and, by isolating risk situations, also aimed at reducing the burden for institutions.

127. The institutions and persons subject to the AML Act are permitted to determine the extent of CDD measures on a risk based approach and take adequate internal measures against ML and TF. In order to be able to make such determinations and define what adequate internal measures should be, the BaFin requires, in circular 8/2005, financial institutions to develop and update institute-specific threat analysis of potential threats with regard to ML/TF (and for credit and financial services institutions also with regard to fraudulent activities). The BaFin requires that the systems of safeguards must be aligned with the size, organization and threat situation of the individual financial institution, as well as its business structure and its customer structure in particular. In consultation with the Central Association of the German Banking Industry (*Zentraler Kreditausschuss*; ZKA) and the German Insurance Association (*Gesamtverband der Versicherungswirtschaft*; GDV), the BaFin and banking industry bodies, the BKA has drawn up an outline paper on TF (catalogue of indicators) that is constantly updated on the basis of intelligence concerning this phenomenon, in particular the latest *modus operandi*, centrally gathered and analyzed by the BKA.

128. In addition, several private sector banking associations (*e.g.* the Association of Public Banks (Verband öffentlicher Banken–VÖB), the Federal Association of Credit Unions and Credit Cooperative Banks (Bundesverband der Volksbanken und Raiffeisenbanken–BVR), and the Federal Association of German Banks (*Bundesverband deutscher Banken–BdB*) which are all members of the ZKA have issued their own guidance papers on internal risk analysis, the latest being the guidance paper of the Federal Association of German Banks (BdB) issued in December 2008. Other Associations (*e.g.* the German Insurance Association–GDV) intend to provide similar guidance for their members.

129. The BaFin focuses most of its supervisory resources on the financial institutions it believes display the highest levels of net risk. Since 2007, the BaFin has operated a system of risk classification for AML/CFT supervision according to which each supervised entity is assigned to one of three risk classes: simplified basic supervision; basic supervision; and enhanced supervision. Each institution is first rated by the BaFin against five key inherent risk criteria. Then, the assessment of the quality of an institution’s AML/CFT measures and safeguards is assessed based largely on the contents of audit reports.

130. The combined result of the threat and the quality of prevention ratings are combined on the following 12-cell-risk classification matrix:

		Quality of AML/CFT-prevention			
		A (high)	B (medium-high)	C (medium-low)	D (low)
Potential threat of ML/TF	3 (high)	3A	3B	3C	3D
	2 (medium)	2A	2B	2C	2D
	1 (low)	1A	1B	1C	1D

131. Each supervised entity is allocated a score on this matrix, ranging from a rating of 1A (low risk–high quality) to a rating of 3D (high risk–low quality). This matrix is then used to determine the extent of supervisory effort.

132. Section 3 of this report contains more details about the RBA for financial institutions in Germany. No formal risk-based approach has been developed for the DNFBPs.

#### ***Progress Since the Last IMF/WB Assessment or Mutual Evaluation***

133. Germany's AML/CFT regime was last assessed in 2004, using the previous assessment methodology. According to the authorities, the following progress has been made to deal with the recommendations contained in that assessment:

- a) **Complete ratification and implementation of international Conventions. Extend current TF provisions to terrorists (as opposed to terrorist organizations):** The UN International Convention for the Suppression of Financing of Terrorism (1999) was ratified in 2004. The Palermo Convention against Transnational Organized Crime was ratified in 2006. Germany claims that its TF provisions do apply to individual terrorists so no further action was required.
- b) **Adopt a new provision in relation to domestic terrorism. Develop comprehensive statistics:** Section 6a of the Banking Act enables the BaFin to stop dispositions with regard to an account of an EU-based person in cases where there is a suspicion that the account relationship is used for terrorist purposes. This Section also allows the BaFin to freeze the assets of such accounts.
- c) **Implement the planned new reporting form is planned. Adopt sanction for failure to report suspicious transactions. More comprehensive statistics:** The detailed technical concept for using electronic transmission reports is in development. The aim is to launch trial operation before the end of 2009. Breaches of the obligation to report are punishable with an administrative fine of up to EUR 100 000 (USD 139 170). Sanctions are also available under



supervisory and administrative law in case of culpable noncompliance with the obligation to report suspicious transactions.

- d) **Improve feedback provisions between the *Land* prosecutor's office and the FIU:** The requirements for the public prosecutors to notify the FIU at the BKA were significantly expanded through the redrafting of the Money Laundering Act in 2008. The reporting requirement was extended to cover criminal proceedings arising from a report of suspected TF. Public prosecutors must send a copy of the indictment, reason for dismissal or verdict to the FIU.
- e) **Render legal mutual assistance notwithstanding the absence of dual criminality. More comprehensive statistics:** Mutual legal assistance is already rendered in spite of the absence of dual criminality in accordance with Section 59 et seq. of the International Assistance in Criminal Matters Act, with the exception of letters rogatory for search or seizure.
- f) **Extend the BaFin supervision to financial enterprises under Section 1 (3) Banking Act (e.g., leasing and factoring):** Leasing and factoring companies are now financial services institutions within the meaning of Section 1(1a) of the Banking Act. All leasing and factoring companies are now also subject to limited supervision by the BaFin. Financial enterprises within the meaning of Section 1(3) of the Banking Act are fully subject to the Money Laundering Act.
- g) **Definition of the term "beneficial owner" could raise concerns. Extend AML/CFT preventive measures in the securities sector to business relationships with foreign counterparts. Enhanced scrutiny on the beneficiary's credit institutions side:** See new Section 1 (6) of the Money Laundering Act (in force since August 21, 2008) for the definition of "beneficial owner."
- h) **Regarding wire transfers, extend provisions to cross-border transfers within the EU:** See Regulation (EC) No. 1781/2006 of November 15, 2006 on information on the payer accompanying transfers of funds, implementing FATF SR VII on wire transfers.
- i) **Investment firms should identify the real customer when performing business relationships with foreign counterparts acting on behalf of clients:** According to German law, all business related to securities trading is considered either banking business or financial services, and as such subject to a licensing requirement. Investment stock corporations and capital investment companies fall under the scope of the Investment Act and are subject to a licensing requirement, too. This ensures that the entire securities sector is regulated and supervised. According to Section 5 (2) number 1 of the Money Laundering Act even in cases of business relationships with other financial institutions, which are qualified as "low risk" and in which simplified due diligence may apply, the identity of the customer always has to be established.
- j) **FIU to establish guidelines with regard to reporting obligations to assist the institutions which must report suspicious activity:** The FIU developed a standardized STR in 2005. However, the use of this standardized STR is not compulsory. The FIU plans to introduce electronic reporting of STRs in the future. The FIU publishes relevant cases that are examples for typologies and methods of ML and TF in annual reports and newsletters, as well as through its public relations work.



- k) **On-site inspections should cover those medium sized or small credit institutions where the STRs are lower than average. More on-site inspections to increase the understanding of the degree of implementation of AML/CFT measures:** In 2007, the BaFin conducted 21 special audits and in 2008, 18 special audits. In 2009, 18 on-site inspections are scheduled. In 2007, the BaFin began to accompany external certified accountants in the context of their follow-up work on the annual audit reports of credit institutions. In 2007, the BaFin conducted 17 audit-accompaniments and in 2008, 14. For the year 2009, 11 audit-accompaniments were planned. However, in Germany, unlike many other countries, the main source of supervisory information is the detailed annual AML/CFT audit reports of all financial institutions supervised by the BaFin. In addition, money remittance services providers and providers of currency business have to forward monthly reports to the BaFin.
- l) **Incorporate specific sanctions regime for non-compliance with the identification requirements in case of suspicious transactions to make enforcement mechanisms more operational in practice:** Breaches of the main provisions relating to identification constitute administrative offenses under either Section 17 (1) or Section 17 (2) of the Money Laundering Act, and are punishable by an administrative fine of up to EUR 100 000 or EUR 50 000 respectively (USD 139 170 or USD 69 585).

## 2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

### Laws and Regulations

#### 2.1. Criminalization of Money Laundering (R.1 & 2)

##### 2.1.1. Description and Analysis

##### *Legal Framework:*

134. Germany has criminalized ML through Section 261 of the CC, by virtue of Article 1 number 19 of the Act on Suppression of Illegal Drug Trafficking and other Manifestations of Organized Crime dated July 15, 1992. The Act and, hence, Section 261 entered into force on September 22, 1992. One of the main aims of this legislation was to improve the legal means for depriving criminals from the proceeds of criminal offenses.

135. Since then, Section 261 of the CC has been subject to a number of amendments, most of which were primarily aimed at extending the list of predicate offenses for ML, particularly to cover criminal offenses related to organized crime. The last amendment took place in August 2009 through the Act on the Prosecution of the Preparation of Serious Violent Acts Endangering the State (*Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten*, GVVG), for purposes of establishing TF offenses as predicate offenses for ML. This amendment was passed after the assessors' on-site visit and entered into force on August 5, 2009 (i.e. within the two months timeframe set out by the FATF). The previous amendment took place in 2008 through the "Act Supplementing the Act to Fight Money Laundering and Terrorist Financing" (*GwBekErgG - Geldwäschekämpfungsergänzungsgesetz*) which had the purpose of implementing the Directive 2005/60/EC of the European Parliament and of the Council of October 26, 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Third EC Money Laundering Directive). This amendment entered into force on August 21, 2008.

##### *Criminalization of Money Laundering (c. 1.1 — Physical and Material Elements of the offense):*

136. Section 261 of the CC provides that "whoever hides an object (*Gegenstand*) which is derived from a predicate offense, conceals its origin or obstructs or endangers the investigation of its origin, its discovery, its forfeiture, its confiscation or its being taken into custody, shall be punished with imprisonment from three months to five years." The second sentence of Section 261 defines predicate offenses for ML to include any serious criminal offense (*Verbrechen*) and a listed number of less serious criminal offenses (*Vergehen*).<sup>24</sup>

<sup>24</sup> The German term "Vergehen" refers to offenses for which the regular minimum punishment laid down by law is a fine or less than one year's imprisonment.

137. The second part of Section 261 provides that whoever (1) procures for one's self or another person or (2) keeps an object indicated in part 1 in custody or uses it for oneself or a third person, shall be punished similarly.

138. The offense covers the material elements of the ML offenses as defined in the Vienna and Palermo Conventions. The "concealment or disguise of the source and location" as well as the "acquisition, possession or use" of property derived from a predicate offense are covered explicitly. While the text of Section 261 of the CC appears narrow with regards to the conduct of concealing, making reference only to the conduct of "concealing the origin" of property, the authorities have demonstrated through well-established doctrine that the text should be interpreted broadly as comprising all forms of concealment required by the Vienna and Palermo conventions.<sup>25</sup>

139. In addition, while Section 261 does not criminalize explicitly the "conversion or transfer" of property derived from a predicate offense, the authorities have stated that the missing conducts would typically be covered by one or more of the conducts that have been criminalized explicitly, and have provided cases as examples that demonstrate convictions for "conversion or transfer."<sup>26</sup>

#### ***The Laundered Property (c. 1.2):***

140. The offense of ML under Section 261 of the CC does not refer to the term "property." Instead, it refers to the term "object" (*Gegenstand*) which is not defined under German law. The authorities stated that the term was especially chosen by the legal drafter precisely because it was not legally defined and because it was meant to cover a broad range of "things involving some kind of economic value." Therefore, the authorities argue that the term covers "any type of property, regardless of a specific value, including for instance movable and immovable property, money, securities and accounts receivables." The authorities also confirmed that use of the expression "derived from an unlawful act" can be interpreted broadly to cover any object that directly or indirectly represents the proceeds of crime and provided doctrine to support these arguments.

#### ***Proving Property is the Proceeds of Crime (c. 1.2.1):***

141. Section 261 of the CC does not specify explicitly whether it is necessary that a person be convicted of a predicate offense to prove the illicit origin of proceeds. While the terms of Section 261 do not appear to suggest that a prior conviction for the predicate crime is necessary when proving that property is the proceeds of crime, assessors received conflicting views regarding this issue. The authorities first made reference to cases where convictions for stand-alone ML were obtained. Some prosecutors explained that, in practice, while it may not be a statutory requirement, it is easier to prosecute and convict a person for ML under section 261 of the CC when there is a prior conviction for the predicate offense, as prosecutors always need to establish a "link" or "connection" between the ML conduct and the predicate offense involved (*i.e.* the court must be convinced of the existence of the predicate offense). This means that the prosecutor will have to prove the specifics of the predicate offense, *e.g.* that the conduct amounted to a designated offense, the perpetrator, and the types of assets that originated from the predicate offense, which is a rather high standard of proof. Most prosecutors and judges met by the assessors indicated that the standard of proof required to link ML to the predicate offense constitutes one of the most difficult obstacles to obtaining a conviction for ML in Germany. In light of the above, assessors conclude that it is

---

<sup>25</sup> Commentary on criminal law by Thomas Fischer, Marginals 19, 29, and 30.

<sup>26</sup> Ruling from the Federal Court of Justice (BGH), dated February 18, 2009, reference no: 1 StR 4/09; Ruling from the Federal Court of Justice (BGH), dated June 24, 2008, reference no: 5 StR 89/08; Ruling from the court of justice (LG) of Ellwangen dated March 30 2007, reference no: 1 S 184/06); Ruling from the Federal Court of Justice (BGH), dated June 21, 1995, reference no: 2 StR 157/95.

not a requirement to have a prior conviction for the predicate offense but that there is some practical advantage if one has been obtained. In addition, the high burden of proof to show that property is the proceeds of crime may hinder, in a practical sense, the pursuit of the ML offense.

***The Scope of the Predicate Offenses (c. 1.3):***

142. The predicate offenses to ML in Germany cover all serious offenses as well as a number of specifically listed less serious offenses under German law. All but two of the FATF-designated categories of predicate offenses are covered under German law. First, while “insider trading and market manipulation,” have been criminalized, there are no offenses under this category that constitute predicate offenses for ML (although the authorities indicated that to pursue the charge of ML they would attempt to charge the perpetrator with fraud, provided that a fraudulent element was present). In addition, “the counterfeiting and piracy of products” is not fully covered, as only the “falsification of documents” is cited as a predicate offense under this category (*e.g.* would apply to false passport, or presenting a document indicating that the seller of a product had a valid patent).

143. In addition, some of the less serious criminal offenses constitute predicate offenses only if certain requirements (aggravating circumstances) are met, namely, that they have been committed with the intention to make a profit, or by a member of a gang founded for the recurrent commission of such an offense. The assessors consider this to be a minor deficiency because it only creates minor practical issues of implementation (*e.g.* may preclude being able to charge perpetrators for one-off minor frauds).

144. Pursuant to Section 261 (1) second sentence of the CC, tax evasion under Section 370 of the Fiscal Code (*Abgabenordnung*, AO) constitutes a predicate offense for ML under German law if it was committed with the intention to make a profit or by a member of a gang founded for the recurrent commission of such an offense.<sup>27</sup>

<b>Predicate Offense under Designated Categories of offenses</b>	<b>German Law</b>
Participation in an organized criminal group and racketeering	Sections 129, 129a and 129b of the CC.
Terrorism, including terrorism financing	Section 129a of the CC (formation of terrorist organizations and financing of terrorist organizations) as well as any less serious offenses committed by a member of a terrorist organization as defined through Section 129a (1) and (2) of the CC. The financing to carry out a terrorist act and the financing of an individual terrorist are covered. under recently incorporated Section 89a (2) number 4 of the CC
Trafficking in human beings and migrant smuggling	Sections 232 (1)(2), 233, 233a (all of them only if committed with aggravating circumstances) and Sections 234 and 234a of the CC.
Sexual exploitation, including sexual exploitation of children	Sections 181a and 232 (1)(2) (both only if committed with aggravating circumstances) and Sections 176a, 176b, 177, 178 and of the CC.
Illicit trafficking in narcotic drugs and psychotropic substances	Sections 29 (1) and (3), 30, and 30a Narcotics Law, Sections 19 (1) and (3) Precursors Control Law.
Illicit arms trafficking	Section 51 and Section 52 (5) Weapon Law.

<sup>27</sup> Note that making tax evasion a predicate offense for ML goes beyond the requirements of the FATF recommendations.

Predicate Offense under Designated Categories of offenses	German Law
Illicit trafficking in stolen and other goods	Section 260a of the CC, Section 374 Fiscal Code.
Corruption and bribery	Sections 332 (1) and (3), 334, and 335 of the CC.
Fraud	Sections 263 (1) – (4) to 265 (only if committed with aggravating circumstances) and Section 263 (5) of the CC (if committed with both aggravating circumstances).
Counterfeiting Currency	Sections 146, 151, 152, 152a (only if committed with aggravating circumstances) and 152b of the CC.
Counterfeiting and piracy of products	Sections 267 of the CC (only applies to falsification of documents)
Environmental crime	Sections 326 (1)(2) and (4), 328 (1)(2) and (4) (both only if committed with aggravating circumstances) and Section 330 (1) and 330a of the CC.
Murder, grievous bodily injury	Sections 176a, 176b, 178, 211, 212, 213, 221 (2), 225 (3), 226, 227, 235 (4) and (5), 251, and 306c of the CC.
Kidnapping, illegal restraining and hostage-taking	Sections 234a, 235 (4), 239 (3), 239a, and 239b of the CC.
Robbery or theft	Sections 242 and 246 (both only if committed with aggravating circumstances) and Sections 249, 250, 251 of the CC.
Smuggling	Section 373 Fiscal Code.
Extortion	Section 253 of the CC (if committed with aggravating circumstances)
Forgery	Sections 267, 269 and 271 of the CC (all only if committed with aggravating circumstances).
Piracy	Section 316c of the CC.
Insider trading and market manipulation	Not a predicate offense for ML

#### ***Threshold Approach for Predicate offenses (c. 1.4):***

145. Germany has taken a combined approach in defining the predicate offenses for ML and this approach meets the requirements of criterion 1.4: Section 261 of the CC defines “unlawful act” as covering any serious offense (*Verbrechen*) as well as certain enumerated less serious offenses (*Vergehen*). Section 12 of the CC provides that “serious offenses” are unlawful acts sanctioned with a minimum of imprisonment of one year or more and “less serious offenses” with a fine or a minimum of imprisonment of less than one year, whereby the minimum sanction is the determining factor for the differentiation. Section 12 further provides that aggravation or mitigation, which is provided under the provisions of the General Part or for especially serious or less serious cases, shall be irrelevant to this classification.

#### ***Extraterritorially Committed Predicate offenses (c. 1.5):***

146. Paragraph 8 of Section 261 of the CC provides that objects which have been obtained through the commission of a predicate offense abroad are equal to those obtained through the commission of a predicate offense in Germany if the act constitutes a criminal offense in the country where it occurred. Therefore, all predicate offenses for ML under German law extend to conducts that occurred abroad, provided that dual criminality is met. It should be noted that the additional requirements (aggravating

circumstances) that need to be met for some of the “less serious offenses” to constitute predicate offenses in Germany, as described under 1.3 above, may also create problems of effectiveness when applying Paragraph 8 of Section 261 of the CC. However, the authorities confirmed that to date, no such problems have arisen.

***Laundering One’s Own Illicit Funds (c. 1.6):***

147. Section 261 of the CC does not distinguish between self laundering and third party laundering. Therefore, the ML provision could in theory be applied to persons who commit the predicate offense. However, paragraph 9 of that same section also provides that a person who has been punished for the commission of the predicate offense may not be punished for ML as well. Accordingly, a person cannot be punished for both the predicate and the ML offenses at the same time. This was confirmed by the authorities, who stated that there can be no conviction for ML if the alleged offender is criminally convicted as a perpetrator of, or aider to, the predicate offense.

148. The authorities indicated that the impossibility of convicting a person for the predicate offense and for ML at the same time derives from fundamental principles of German domestic law, such as the general principle of express immunity from criminal proceedings for instances in which perpetrators assist themselves after the fact (*Selbstbegünstigungsprinzip*), which is granted by section 257 and 258 of the CC. According to this principle, an offender (*i.e.* the one having committed the predicate offense) cannot be additionally and separately punished for a “post-offense behavior” that relates to the proceeds of his or her own crime. This implies that one punishable act (the predicate offense) includes another concurring act (the concealing or disguising of property items that derive from the predicate offense’s perpetrator) and that the penalty set forth for the punishable act is deemed to cover the entire unlawfulness of the offenders' act.

149. Basing its considerations specifically on section 261 (9) of the CC, the Federal Court of Justice (BGH) has ruled<sup>28</sup> that the ML offense was not intended to punish perpetrators twice, once for the predicate offense and once for the act of ML. It also stated that the provision of section 261 (9), second sentence, of the CC, which has been worded as personal grounds for exemption from punishment for an unlawful act, is in fact a concurrent provision of the law excluding criminal liability for ML in all cases in which the perpetrator is already punishable by law due to being involved in the predicate offense.

150. However, these rulings do not indicate explicitly that self-laundering is contrary to a fundamental principle of German law and some practitioners met by the assessors did not have a uniform view as to whether there is a fundamental principle on the subject.

151. The above explanations raise serious doubts regarding the autonomy of the ML offense under German law and contribute to explain some of the difficulties in applying the ML offense in Germany. ML does not always involve instances where perpetrators assist themselves after a fact. In particular, when the laundering activity does not simply amount to the mere possession or use, but also involves the transfer or the concealment and disguise through the financial system – an additional damage to further rights than the one already caused by the predicate offense – as well as an additional social danger (to the soundness and the integrity of the financial system) can be envisaged autonomously and therefore could deserve a separate punishment.

152. While the ML conduct in a self laundering case could be investigated, and even punished if no punishment has been applied for the predicate offense, due to the principles of mandatory investigation and mandatory prosecution that govern German criminal procedures, it is more likely for a self launderer to be

---

<sup>28</sup> Judgment published in New Journal for Penal Law (*Neue Zeitschrift für Strafrecht*, NStZ) 2003, p. 499 (500).



first investigated, prosecuted, and punished for the commission of the predicate offense. As a result, in cases of self laundering, it is very likely that the ML conduct will remain unpunished. This was confirmed by the majority of the prosecutors that met with assessors.

153. The authorities have asserted that, in cases of self laundering, the ML conduct would typically be considered as an aggravating circumstance when applying the punishment for the commission of the predicate offense and that this would result in a more severe punishment for the offender. However, based on the above, assessors must conclude that it was not established that the offense of ML can apply to persons who commit and are convicted of the predicate offense. In addition, it was not established that the impossibility to apply the ML offense to persons who commit and are convicted of the predicate offense is supported by principles that amount to fundamental principles under the FATF's standards.

***Ancillary offenses (c. 1.7):***

154. Ancillary offenses are defined in the general section of the CC and apply to all offenses, including ML. All ancillary offenses provided for under the Vienna and Palermo conventions are covered under German law.

155. Section 23 of the CC provides that attempts to commit a "serious offense" (*Verbrechen*) are always criminalized, whereas attempts to commit a "less serious offense" (*Vergehen*) are only criminalized if specifically provided for in the law. In the case of ML, which is a less serious offense, Section 261(3) specifically provides that any attempt to commit ML is a criminal offense. The conducts of "intentionally inciting another to commit an unlawful act" and "intentionally assisting another in the commission of an intentional crime" are punished with the same punishment as the perpetrator. Assistance should be interpreted in a broad sense, therefore, covering aiding and abetting, facilitating, and counseling the commission.

156. The conducts of "declaring one's willingness, accepting the offer of another, or agreeing with another to commit a "serious criminal offense" (*Verbrechen*)" are punished as attempts to commit a crime. However, since the basic ML offense is a "less serious criminal offense" (*Vergehen*), the "attempt to participate in it" is not covered by this provision.

157. Conspiracy to commit ML, in the sense generally known in common law systems (that envisage conspiracy also in the case of an agreement of only 2 persons), is not to be found under German criminal law. Germany has a civil-law based criminal system and the basic concepts of such a system do not provide that such behavior constitutes punishable criminal conduct. Instead, Section 129 of the CC provides that it is a criminal offense to "form a group, the objectives or activity of which are directed towards the commission of crimes", including ML. This is in line with the Vienna and Palermo Conventions (Article 3 (1), c, iv and Art. 6, (1), b, ii, respectively, which require the establishment of an offense either for conspiracy or association, subject to the constitutional/basic concepts of the jurisdiction's legal system).

158. A group within the meaning of sections 129 et seq. is deemed to be an organizational combination of at least three persons, designed to exist for a certain period of time, where – with subordination of the will of the individual to the will of the group as a whole – the members pursue common goals, while standing in such relation to one another that they feel themselves to be a uniform cluster.<sup>29</sup>

---

<sup>29</sup> Munich Commentary on the Criminal Code (CC) (*"Müncher Kommentar zum StGB"*), Vol. 2/2, 1st. edition 2005 CC; Author: Miebach/Schäfer, Section 129 a of the Criminal Code: formation of terrorist groups; margin ref. 22-34.



159. Other offenses that cover certain aspects of ancillary conducts with respect to ML include “assistance in avoiding prosecution or punishment” pursuant to Section 258, “assistance given in official capacity” pursuant to Section 258a, “handling stolen goods” pursuant to Section 259 and “handling of stolen property committed with aggravating circumstances” pursuant to Section 260 and 260a of the CC.

***Additional Element — If an act overseas, which does not constitute an offense overseas but would be a predicate offense if it occurred domestically, leads to an offense of ML (c. 1.8):***

160. As a general principle, conduct criminalized in Germany and abroad constitutes a predicate offense to ML under German law. However, Sections 5 and 6 of the CC provide for certain exceptions to this rule and apply German law even in the absence of dual criminality.

161. According to Section 5 of the CC, Germany’s criminal law is applicable, regardless of the law of the place where the act was committed, to certain forms of sexual abuse of children and certain environmental crimes, as well as to the offenses of “child stealing,” among other unlawful acts committed abroad and considered to be against domestic legal interests. Furthermore, Section 6 of the CC provides that Germany’s criminal law is applicable, regardless of the law of the place where the act was committed, to piracy, trafficking in human beings and migrant smuggling, illicit trafficking in narcotics and counterfeiting of currency or securities, among other unlawful acts committed abroad and considered to be against international legal interests.

162. Accordingly, for all predicate offenses committed abroad and listed in Sections 5 or 6 of the CC, a conviction for ML may be obtained under German law even if the predicate offense is not criminalized in the country where it occurred.

***Liability of Natural Persons (c. 2.1):***

163. Pursuant to Section 15 of the CC, only “intentional” acts are considered crimes under German law unless a specific provision expressly criminalizes negligence. Section 261 (1) of the CC applies to any natural person who commits any of the acts constituting ML. The conduct requires the perpetrator to know that the objects being dealt with derived from an unlawful act, and prosecutors must prove this beyond reasonable doubt.

164. ML pursuant to Section 261 (1) and (2) generally requires intentional commission of the act by the perpetrator. However, Section 261 (5) also provides for criminal liability of negligent ML if the perpetrator “recklessly did not know that the objects in question stem from the commission of a predicate offense.” This considerably lightens the burden of proof placed on the prosecution and goes beyond the requirements of the FATF 40+9 Recommendations.

165. Whereas Section 261 (2) (keeping proceeds of crime in custody or using them) requires that the perpetrator knew at the time of receipt that the origin of the object is criminal, no specific knowledge with respect to the property is required for the acts of Section 261 (1) (hiding proceeds of crime, concealing its origin or obstructing or endangering the investigation of its origin, its discovery, its forfeiture, its confiscation or its being taken into custody). However, as already stated above, Section 261 (5) provides that a person may be held criminally liable for ML pursuant to both Sections 261 (1) and (2) even when the person did not know, due to negligence, that an object was the proceeds of crime. This would imply that in all other cases, Section 261 (1) and (2) require that the perpetrator knew or should have known that the object in question has been derived from the commission of a predicate offense.

***Inference of the Mental Element of the ML offense (c. 2.2):***

166. The law permits the intentional element of the offense of ML to be inferred from objective factual circumstances. Article 261 of the Criminal Procedures Code (CPC) establishes the principle of free evaluation of evidence. This principle states that the facts and circumstances related with the purpose of the proceeding may be admitted by any means of evidence, except for the exceptions provided for in the laws. A means of evidence is admitted if it refers directly or indirectly to the purpose of the investigation and is useful for revealing the truth. Accordingly, the mental element of the offense may be inferred through *indicia*, constituted by external facts and circumstances that are proved in the proceedings. The authorities have provided case law where the courts have upheld these principles.<sup>30</sup>

***Liability of Legal Persons (c. 2.3); Criminal Liability of Legal Persons should not preclude possible parallel criminal, civil or administrative proceedings (c. 2.4):***

167. Under German law, legal persons are not subject to criminal liability. The German legal system follows the principle of “*societas delinquere non potest*” (no criminal liability for legal entities) which is based on the long standing criminal law principle of “*nulla poena sine culpa*” (*i.e.* no punishment without guilt), and is characterized by an individual and personal conception of criminal liability. The arguments that derive from these principles are that legal persons are unable to act in a criminal law sense due to the absence of will; that, in the absence of will, legal persons are not capable of being considered guilty in a criminal law sense; and that, without guilt, no criminal punishment may be imposed on legal persons. These notions have been upheld by Germany’s Federal Constitutional Court<sup>31</sup> and are, therefore, considered fundamental principles of domestic law.

168. Notwithstanding these principles, legal persons involved in ML may be subject to administrative fines and the fines can also contain a component aimed at recovering the profit from the criminal activity. The level of regulatory fine that can be imposed is up to EUR 1 million (USD 1.4 million) pursuant to Sections 30 and 130 of the Administrative offense Act. In addition, pursuant to Section 17 (4) of the Administrative Offenses Act, the fine shall exceed the financial benefit that the perpetrator has obtained from the commission of the regulatory offense. The authorities have provided evidence of recent corruption cases where the statutory fine was exceeded up to EUR 75 million (USD 104 million)<sup>32</sup>. If the case involves a criminal offense, the administrative fine may be imposed by the criminal court.

169. Section 30 specifies that, an administrative fine may be imposed on a legal person where someone acting on its behalf has committed a criminal offense or a regulatory offense as a result of which duties incumbent on the legal person have been violated, or where the legal person has been enriched or was intended to be enriched. Where an administrative fine is incurred by a legal person or an association of persons, a forfeiture order with respect to the same offense is precluded against such person or association of persons, as the fine is meant to deprive the person of the benefit of the crime.

<sup>30</sup> Rulings of the Federal Court of Justice in Criminal Law Matters (*Entscheidungen des Bundesgerichtshofes in Strafsachen*, BGHSt) 36, p. 9 et seq. (HIV Infection).

<sup>31</sup> Ruling handed down by the Federal Constitutional Court on October 25, 1966; reference no: 2 BvR 506/63 and Ruling most recently handed down by the Federal Constitutional Court (BVerfG) on the Treaty of Lisbon (ruling dated June 30, 2009 (2 BvE 2/08), paragraph no. 364.

<sup>32</sup> Recent cases where the statutory fine was exceeded were: the MAN case (corruption case, EUR 108 million or USD 150 million) and Siemens (corruption case, EUR 0.93 billion or USD 1.3 billion), among others (one of them involving EUR 2 million or USD 2.8 million and the other one, EUR 4.5 million or USD 6.3 million).

170. Other laws provide for administrative sanctions against legal persons (*i.e.* revocation, suspension or termination of the legal person's license, exclusion from public contract, etc.).

***Sanctions for ML (c. 2.5):***

171. ML is sanctioned with imprisonment of three months to five years if committed intentionally and with imprisonment of up to two years or a fine if committed negligently.

172. The negligent type of ML requires a lower standard of proof and could therefore contribute to achieving more convictions. In recent years, the amount of convictions for negligent ML (Section 261 (5)) has grown significantly in Germany, amounting to nearly half of the total number of convictions for ML per year.

173. In aggravated circumstances, *i.e.*, when the perpetrator acts with the intention to make a profit or as part of an organized group whose purpose is the continued commission of ML, the applicable sanction is six months to ten years. Both the basic and the aggravated offense therefore constitute a less serious crime (*Vergehen*) under the CC. The statistics below show that only a small number of convictions per year are connected with the aggravated type of ML (Section 261 (4)). This is consistent with the statistics showing that only a small number of convictions involve more than two offenders.

174. Persons held criminally liable for "inciting another" to commit ML pursuant to Section 26 of the CC are sanctioned to the same extent as the main perpetrator of the offense. Attempted acts of ML may be sanctioned to the same extent as completed acts, but the court may impose no more than three quarters of the statutory maximum term pursuant to Section 49 of the CC. The sanctions applicable to the offense of "assisting another" to commit ML pursuant to Sections 27 and 49 are basically the same as for the principal offense, but the court is obliged to reduce them to no more than three quarters of the statutory maximum term.

175. Pursuant to Section 40 of the CC, a fine is imposed on a *per diem* basis, and amounts to a minimum of five *per diems* and, if the law does not provide otherwise, a maximum of 360 *per diems*. The ML offense under Section 261 of the CC does not provide a lower maximum, so the 360 *per diems* apply as the top of the range. The court determines the amount of the *per diem*, taking into consideration the personal and financial circumstances of the perpetrator. In doing so, it takes as its starting point the perpetrator's average net income per day. The minimum daily rate is fixed EUR 1.00 (USD 1.39) and a maximum of EUR 30 000 (USD 41,751). In determining the daily rate the income of the perpetrator, the perpetrator's assets and other bases may be estimated. The number and amount of the daily rates shall be indicated in the decision.

176. While the CC permits the imposition of "imprisonment" or "fines," it generally does not allow for these sanctions to be applied jointly. However, pursuant to its Section 41, if by the act the perpetrator was enriched, or tried to be enriched, then a fine, which otherwise would have been inapplicable or only optional, may be imposed as collateral to imprisonment, if it is appropriate, taking into consideration the personal and financial circumstances of the perpetrator.

177. In accordance with Section 56 of the CC, upon a sentence for an offense of imprisonment of no more than one year the court shall suspend the execution of the punishment and grant probation if it can be expected that the sentence will serve the convicted person as a warning and the person will commit no further crimes in the future even without the influence exerted by serving the sentence. The court must take into account the personality of the convicted person, previous history, the circumstances of the criminal act, conduct after the act, living conditions and the effects which can be expected as a result of the suspension. The court may also suspend the execution of a term of imprisonment which does not exceed

two years and grant probation if a comprehensive evaluation of the act and personality of the convicted person reveals the existence of special circumstances. In making the decision the efforts of the convicted person to make restitution for the harm caused by the act should be particularly considered.

178. As stated above, the offense of ML is criminalized in Germany as a less serious crime (*Vergehen*). In effect, when compared to some of the serious offenses (*Verbrechen*) in the assessed jurisdiction, the level of sanctions for ML does not seem to be proportionate and dissuasive (*i.e.* formation of terrorist organizations = 1–10 years imprisonment, trafficking human beings = 6–10 years imprisonment, trafficking stolen goods = 1–10 years imprisonment, counterfeiting = 1–10 years imprisonment). However, when compared with other less serious offenses (*Vergehen*) in the assessed jurisdiction, the level of sanctions appears more proportionate (*i.e.* robbery, fraud, breach of trust, falsification of documents and racketeering are all sanctioned with a fine or imprisonment up to five years).

179. The sanctions for basic ML offenses are lower relative to the sanctions for ML offenses in some of the FATF countries (*i.e.*, Argentina = 2–10 years imprisonment, Brazil = 3–10 years imprisonment, Mexico = 5–15 years imprisonment, Italy = 4–12 years imprisonment, United States = fine and/or imprisonment up to 20 years or both, United Kingdom = fine, imprisonment up to 14 years or both) but nearer relative to ML offenses in other FATF countries (*i.e.* Finland = fine or imprisonment up to 2 years, Japan = fine, imprisonment up to 5 years or both).

180. The sanctions applied for ML, with a focus on imprisonment or youth custody are shown in the following tables. The tables reflect that the majority of convictions for ML do not involve prison sentences and that the vast majority of convictions involving prison sentences are suspended. The tables also reveal that there were comparatively few convictions for ML in aggravated circumstances under Section 261 (4) of the CC (*i.e.* conducts carried out with the intention to make a profit or as part of organized crime).

**Statistical Table 12: Imprisonment or youth custody sanctions for those convicted of offenses pursuant to Section 261 of the Criminal Code**

Year	Total convictions	Imprisonment or youth custody of more than ... up to (and including) ...							
		Total imprisonment	up to 1 year		1–2 year(s)		2–3 years	3–5 years	5–10 years
			without	with	without	with			
			sentence suspended		sentence suspended				
2004	112	65	-	41	5	12	4	3	-
2005	97	51	1	29	2	14	3	2	-
2006	216	52	-	34	3	12	1	1	1
2007	603	106	2	68	3	27	3	3	-
2008	608	113	3	79	4	20	6	1	-
For those convicted of offenses pursuant to Section 261 (1) of the Criminal Code									
Year	Total convictions	Imprisonment or youth custody of more than ... up to (and including) ...							
		Total imprisonment	up to 1 year		1–2 year(s)		2–3 years	3–5 years	5–10 years
			without	with	without	with			
			sentence suspended		sentence suspended				
2004	86	52	-	34	5	8	3	2	-
2005	62	33	1	19	2	8	2	1	-
2006	100	32	-	18	3	10	1	-	-

<b>Statistical Table 12: Imprisonment or youth custody sanctions for those convicted of offenses pursuant to Section 261 of the Criminal Code</b>									
<b>2007</b>	264	61	2	35	2	19	2	1	-
<b>2008</b>	248	75	1	54	3	13	3	1	-
For those convicted of offenses pursuant to Section 261 (2) of the Criminal Code									
Year	Total convictions	Total imprisonment	Imprisonment or youth custody of more than ... up to (and including) ...						
			up to 1 year		1–2 year(s)		2–3 years	3–5 years	5–10 years
			without	with	Without	with			
			sentence suspended		sentence suspended				
<b>2004</b>	6	5	-	3	-	1	1	-	-
<b>2005</b>	6	5	-	1	-	3	1	-	-
<b>2006</b>	5	3	-	3	-	-	-	-	-
<b>2007</b>	19	6	-	6	-	-	-	-	-
<b>2008</b>	19	6	1	4	-	1			
For those convicted of offenses pursuant to Section 261 (4) of the Criminal Code									
Year	Total convictions	Total imprisonment	Imprisonment or youth custody of more than ... up to (and including) ...						
			up to 1 year		1–2 year(s)		2–3 years	3–5 years	5–10 years
			without	with	Without	with			
			sentence suspended		sentence suspended				
<b>2004</b>	6	4	-	2	-	1	-	1	-
<b>2005</b>	9	5	-	2	-	2	-	1	-
<b>2006</b>	17	10	-	6	-	2	-	1	1
<b>2007</b>	23	11	-	2	1	5	1	2	-
<b>2008</b>	25	10	-	1	1	5	3	-	-
For those convicted of offenses pursuant to Section 261 (5) of the Criminal Code									
Year	Total convictions	Total imprisonment	Imprisonment or youth custody of more than ... up to (and including) ...						
			up to 1 year		1–2 year(s)		2–3 years	3–5 years	5–10 years
			without	with	Without	with			
			sentence suspended		sentence suspended				
<b>2004</b>	14	4	-	2	-	2	-	-	-
<b>2005</b>	20	8	-	7	-	1	-	-	-
<b>2006</b>	94	7	-	7	-	-	-	-	-
<b>2007</b>	297	28	-	25	-	3	-	-	-
<b>2008</b>	316	22	1	20	-	1	-	-	-

Source: Federal Statistical Office (*Statistisches Bundesamt*) (ed.), *Strafverfolgung* (Prosecution). The figures for the years up to and including 2006 refer to the so-called "old" *Länder*; in other words the Federal Republic of Germany prior to re-unification, including greater Berlin. From 2007, the figures represent all of Germany.

181. The sanctions set forth for ML in the case of natural persons are too lenient (particularly in the case of basic ML). Given the low end range of sanctions, the fact that the majority of sanctions imposed by the courts do not involve prison sentences, and that the vast majority of sanctions involving prison sentences are suspended, the assessors conclude that the basic offense of ML is not subject to effective, proportionate, and dissuasive sanctions. Germany has not provided statistics on the application of

administrative fines to legal persons and assessors were, therefore, unable to evaluate the effectiveness in this area.

### Statistics (R.32)

#### Reported Offenses (Selected)

	2003	2004	2005	2006	2007	Total
Total reported offenses	6 572 135	6 508 604	6 287 780	6 203 074	6 195 622	31 767 215
Drug related	258 143	285 914	278 950	257 253	250 895	1 331 155
Economic crimes	86 249	81 135	89 224	95 887	87 934	440 429
Money laundering <sup>33</sup>	745	776	2 073	2 997	3 923	10 514

Source: Bundeskriminalamt, Police Crime Statistics 2003-2007.

#### Preliminary Criminal Investigations by State Prosecutors for ML (2004- 2008)<sup>34</sup>

Year	2004*	2005	2006	2007	2008	Total
Preliminary Investigations <sup>l</sup>	4 770	6 692	9 929	13 593	10 478	45 462
Number of STRs filed	8 062	8 241	10 051	9 080	7 349	42 783

Source: Federal Statistical Office (*Statistisches Bundesamt*) (ed.), *Fachserie 10, Rechtspflege Staatsanwaltschaften* (series 10 on the administration of justice by the state's prosecution). The figures for 2004–2007 refer to the entire area of the Federal Republic of Germany. \*2004 without information on Schleswig-Holstein. No information is available for 2003. For the year 2004, no information has been made available by the *Land* Schleswig-Holstein. For all other years, the figures cited refer to the entire area of the Federal Republic of Germany.

#### Charges for ML by Section

	2004	2005	2006	2007	2008	Total
Section 261 (1) (hiding, concealing, obstructing, or endangering)	116	87	133	336	359	1 031
Section 261 (2) (keeping or using)	7	7	7	27	21	69
Section 261 (4) (aggravated type)	7	14	19	24	28	92
Section 261 (5) (negligent type)	14	21	100	321	358	814
Total	144	129	259	708	766	2 006

182. The number of charges is always lower than the number of preliminary investigations, as the investigations do not always confirm the suspicion of a criminal offense against the suspect. The vast majority of all investigations concerning ML are in fact suspended for that reason. In addition, due to the limitations in punishing a person for the predicate offense and for ML at the same time (section 261 subsection 9 of the CC), criminal proceedings initiated on the basis of an STR for ML are usually discontinued and new proceedings are initiated for the predicate offense. As a general rule, after discontinuing a criminal proceeding for ML and opening a new criminal proceeding for the predicate offense, the competent public prosecutor changes. As a result, no conclusions can be drawn as to how

<sup>33</sup> These statistics are based on the status of the reported offense at the time that the case is concluded by the police, and the statistical classification is based on the crime category with the most serious punishment available. Moreover, the initial report of the crime to the police may not always be based on an STR or the prosecutor may have dropped the charge of ML if the case was related to self-laundering. Accordingly, this classification tends to relate to the underlying predicate crime rather than ML, and it is difficult to reconcile with the number of filed STRs.

<sup>34</sup> These statistics are also difficult to reconcile with the number of STRs filed, due mainly to the way that these data are compiled. Although each STR triggers the need to carry out a preliminary criminal investigation for ML, the statistical classification system is based on matters other than the initial filing of the STR.



many proceedings initiated on the basis of an STR resulted in the commencement of an action or a conviction for a predicate offense.

183. The statistics do not allow any conclusions to be drawn concerning the reasons why the number of charges for ML increased from 2005 to 2006 and Germany was unable to provide a reasonable explanation regarding this increase.

**Statistical Table 13: Convictions for ML**

	2004	2005	2006	2007	2008	Total	%
Section 261 (1)	86	62	100	264	248	760	46%
Section 261 (2)	6	6	5	19	19	55	3%
Section 261 (4)	6	9	17	23	25	80	5%
Section 261 (5)	14	20	94	297	316	741	45%
Total	112	97	216	603	608	1,636	100%
As percentage of charges laid	78%	75%	83%	85%	79%	82%	

184. The statistics do not allow any conclusions to be drawn concerning the reasons why the number of convictions for money laundering increased from 2005 to 2006 and Germany was unable to provide a reasonable explanation regarding this increase.

**Sanctions for ML**

	2004	2005	2006	2007	2008	Total
Juvenile sanctions	2	4	7	17	17	47
Imprisonment and youth custody (of which suspended)	65 (53)	51 (43)	52 (46)	106 (95)	113 (99)	387 (336)
Average length of sentence	N/A	N/A	N/A	N/A	N/A	N/A
Number of cases in which fines were issued	45	42	157	480	476	1 200
Average fine	N/A	N/A	N/A	N/A	N/A	N/A
Total number of persons on whom sanctions were imposed	112	97	216	603	608	1 636

185. The increases recorded for ML charges, convictions, and sanctions from 2006 to 2007 can be partially explained by the fact that the information provided for the years 2004 until 2006 exclusively represents the situation of the so-called "old" *Länder*, i.e. the Federal Republic of Germany prior to reunification, including greater Berlin. Data for the entire Federal Republic, i.e. including the *Länder* of Brandenburg, Mecklenburg-Western Pomerania, Saxony, Saxony-Anhalt and Thuringia, has only been recorded since 2007.

186. No information can be provided on the average length of the sentences handed down since the statistics on criminal prosecution only record the term of prison sentences in groups (less than 6 months, 6 months, more than 6 to 9 months, more than 9 months to 1 year, more than 1 to 2 years, more than 2 to 3 years, more than 3 to 5 years, more than 5 to 10 years, more than 10 to 15 years, and life imprisonment).

187. The average amount of fines imposed cannot be determined for the same reason, since these are only captured in groups (5 to 15, 16 to 30, 31 to 90, 91 to 180, 181 to 360, and 361 daily rates and over). It should be noted in this context that the amount of a fine, as an absolute number, does not allow any conclusions to be drawn as to the seriousness of the offense since the total fine levied is a factor of the number of daily rates imposed.

188. In accordance with the general practice in Germany for similar crime types, the vast majority of imposed sanctions are fines, and the vast majority of custodial sentences for ML are suspended. The



authorities indicated that these data do not show the full picture relating to how offenders are dealt with and that some offenders may have been sentenced to custodial sentences for other more serious charges.

**Statistical Table 14: Acquittals on ML Charges by Section**

	2004	2005	2006	2007	2008	Total
Section 261 (1) offenses	7	5	7	8	11	38
Section 261 (2) offenses	0	0	1	4	0	5
Section 261 (4) offenses	0	3	0	0	1	4
Section 261 (5) offenses	0	0	1	1	3	5
Total	7	8	9	13	15	52
Acquittals as percentage of charges laid	6%	6%	3%	2%	2%	3%

**Number of Accused Involved in ML Investigations in 2008**

Accused involved in concluded investigations	Number	Percentage
1 accused	8,361	(79.8%)
2 accused	1,550	(14.8%)
3 accused	349	(3.3%)
4-10 accused	209	(2.0%)
11 or more accused	9	(0.1%)
Total number of persons subjected to investigation	13 708	

Based on total number of cases investigated and concluded in 2008 (13 708).

**Prosecutions and Convictions for Main Predicate Crimes**

	2007		2008	
	Prosecutions	Convictions	Prosecutions	Convictions
263-265b of the CC, Fraud	206 995	170 264	199 850	163 987
267-281 of the CC, Document forgery	26 691	22 486	25 068	20 909
Offenses under the Fiscal Code (tax and customs offenses)	17 194	15 573	18 153	16 448
266-266b of the CC, Breach of fiduciary duty	12 738	10 383	11 878	9 750
Offenses under the Narcotics Act	64 237	57 116	68 519	61 256
283-283d of the CC, Insolvency offenses	2 055	1 636	1 984	1 570
242-244a of the CC, Theft	181 729	147 148	177 550	152 519
Alien smuggling under sections 96 and 97 of the Residence Act	1 123	947	1 049	885

189. Where the fines levied against legal persons are concerned, the statistics published by the Federal Statistical Office on the administration of justice do not distinguish between the facts and circumstances on which such fines are based. Thus, it is not possible to provide any information on the number of instances in which a fine was levied against legal persons for ML.

190. A preliminary analysis by IMF staff of the number of ML convictions secured in 23 countries assessed under the FATF 2004 Methodology for which data are available suggests initially that 327 convictions per year in Germany is an impressive result despite the fact that in many cases the predicate offense rather than the ML offense is pursued. Germany has the second highest annualized number of convictions in the group of countries studied. The result also appears credible when compared to the 18 countries assessed as LC or higher, when the convictions are normalized by reference to either population or GDP. This is illustrated in the following table:

**Statistical Table 15. ML Conviction Statistics for Selected Countries**

Indicator	Average of 23 assessed countries*	Average of 18 countries assessed LC or higher*	Germany (Average for the years 2004 through 2008**)
Average number of convictions for ML each year	97.4	120.6	327.2
Average number of ML convictions each year per million of population	0.05	3.48	4.40
Average number of ML convictions each year per USD billion of GDP	0.01	0.13	0.14

\* The countries are: Albania, Australia\*, Belgium\*, Canada\*, Colombia\*, Cyprus\*, Denmark\*, Dominican Republic, Fiji\*, Greece, Iceland\*, India, Ireland\*, Norway\*, Portugal\*, Russia\*, Slovakia\*, Spain\*, Sweden\*, Switzerland\*, Thailand, U.K.\*, and U.S.A.\* (\* indicates assessed as LC or higher.)

\*\* The data for the years prior to 2006 has been analyzed using estimates of population and GDP for those years for the equivalent of pre-unification West Germany.

### *Analysis of Effectiveness:*

191. The CC is the centerpiece of German criminal law and, as such, benefits from a rich experience of doctrinal analysis and case law that facilitates its interpretation. In addition, the institutional foundations of the criminal system are solid and comprise extremely well informed officials that guarantee a reasonably uniform application of the law. These are major advantages of the German criminal law system which contribute to its general effectiveness.

192. Germany's criminal justice system appears to achieve effective outcomes for dealing with profit motivated crimes. The authorities assured the assessment team that offenders are convicted and sentenced on the basis of the most serious crime, and deprived of their assets (see commentary under Recommendation 3). However, the specific charge of ML is not the primary tool for achieving this outcome. Moreover, the authorities were unable to point to any statistics that demonstrated the link between the investigations into ML and subsequent convictions and sanctions for other crimes.

193. Germany's choice to categorize the ML offense as a "less serious offense" appears to entail a number of disadvantages. In addition to sending a weak message on the relevance that German criminal law assigns to this offense, this categorization offers prosecutors and judges a weak range of sanctions to apply as a punishment for the ML conduct. Moreover, it opens the path to the suspension of the execution of the punishment and the benefit of probation to a large number of ML offenders. In effect, it is clear that the majority of sanctions applied for ML do not involve prison sentences, and that the vast majority of sanctions involving prison sentences are suspended.

194. This said, the statistics that are available reflect that German courts obtain a high number of convictions for ML per year and that there is a high percentage of convictions for ML vis-à-vis the number

of charges laid. However, based on the low- end range of sanctions, the fact that most sanctions do not involve prison sentences, and because the vast majority of sanctions involving prison sentences are suspended, the assessors concluded that the sanctions were not effective, proportionate and dissuasive.

195. In addition, the authorities have generally indicated that not much emphasis is being placed in prosecuting serious ML as an effective tool to tackle serious organized crime. This is supported by the statistical evidence, which indicates that most cases under investigation involved only a single perpetrator, and only 5% of convictions obtained relate to section 261(4) (i.e. ML conduct carried out for profit or as part of organized crime). Accordingly, more efforts need to be placed at raising awareness on the opportunity that ML investigations and convictions represent to the general fight against organized crime.

196. In this regard, prosecutors confirmed that the majority of cases that complete the preliminary investigations (*i.e.* the “clearing process”, as further described under Recs. 27-28) successfully are usually cases involving conducts of “self laundering.” In such cases, however, given that self launderers cannot be punished for the predicate offense and the ML offense concurrently, the common practice is usually to pursue the investigation with a focus on the predicate offense and drop the investigation into the ML conduct. This is supported by the statistics provided by the authorities, which reveal that the vast majority of proceedings initiated for ML do not result in ML charges. An exception to this practice would be those “self laundering cases” in which the evidence gathered to prove the ML conduct was stronger than the one for the predicate offense, in which cases, a prosecution for ML may be easier to support. An example of this appears to be the ML cases derived from phishing conducts,<sup>35</sup> which according to prosecutors have been increasing greatly in recent years, and which usually lead to prosecutions for the ML offense (usually the negligent type under Section 261 (5) of the CC). This may explain the increase in the number of ML convictions where Section 261 (5) was applied. These have grown to 52% of total convictions in the latest year, and account for 45% of all convictions obtained. Pursuing low-end ML conduct is also consistent with the fact that the majority of ML cases involve single perpetrators, that the sanctions imposed were low and that the majority of sanctions involving imprisonment were suspended. Further evidence about the low end level of cases pursued is that the average amount claimed per proceeding by the state for forfeiture and confiscation has dropped off by more than 50 percent in the latest year that data are available for (see discussion under R.3).

197. Prosecutors also explained that, in cases where the perpetrator of the ML offense is someone different than the perpetrator of the predicate offense, the focus of the investigation also tends to be placed on the predicate offense. In these cases, the ML conduct usually tends to be prosecuted as “participation” in the commission of the predicate offense, which apart from being easier to prove than the ML conduct, usually carries a higher punishment than the one envisaged for ML (*i.e.* the same punishment as the perpetrator). As described above, this is due to the rather high burden of proof required in proving that property is the proceeds of crime (*i.e.* the need to establish a “link” or “connection” between the ML conduct and the predicate conduct, which is the essence of the clearing process) and the fact that ML is categorized as a “less serious offense” and, therefore, carries a rather low punishment vis-à-vis most predicate offenses.

198. In addition, while predicate offenses include a range of offenses in most of the designated categories, the requirements that have to be met for certain less serious criminal offenses to be included as a predicate offense to ML (*i.e.* committed with the intention to make a profit or by a member of a gang founded for the recurrent commission of such an offense) may be preventing a much broader use of the ML offense in Germany. Moreover, such requirements may theoretically also restrict Germany’s capacity

---

<sup>35</sup> Phishing is understood as the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

to provide certain forms of international cooperation where dual criminality is required (*i.e.* extradition with non-EU jurisdictions).

199. Due to the absence of statistics on the number of administrative fines effectively applied to legal persons assessors could not determine that sanctions are effectively applied to legal persons.

200. In summary, it seems clear that, despite the high number of convictions for ML, Germany is not using the ML offense effectively to tackle serious profit motivated crime. This does not mean that such conducts are not being punished, as they are usually punished through the application of serious offenses that carry more severe punishments. However, it does reveal that the ML offense is not fully serving its purpose. The assessors are of the view that this situation may be related to the limitations of the offense described above and that the effective implementation of the offense could be improved if such limitations were removed.

### 2.1.2. Recommendations and Comments

201. In order to comply fully with Recommendations 1 and 2, Germany should:

- Amend the CC to re-categorize the offense of ML as a serious crime and to raise the range of sanctions to make them effective, proportional and dissuasive, relative to other serious offenses in the CC.
- Increasing the minimum and maximum ranges of sanctions applicable to ML, consistent with the level of penalties for serious offenses in Germany.
- Reduce the burden of proof that is deemed necessary to prove that property is the proceeds of crime.
- Create predicate offenses for ML for the following two categories of offenses: “insider trading and market manipulation,” and “counterfeiting and piracy of products.”
- Amend the CC to ensure that predicate offenses for ML include a range of offenses in each of the designated categories of offenses without having to meet the additional requirement (aggravating circumstances) that the offense is committed to make a profit, or by a member of a gang founded for the recurrent commission of such an offense.
- Allow for the concurrent prosecution of and sanctioning for self laundering and for the commission of the predicate offense.
- Raise awareness among prosecutors and law enforcement agencies on the opportunity that ML investigations and convictions represent to the general fight against organized crime.
- Maintain statistics on the sanctions applied to legal persons.

### 2.1.3. Compliance with Recommendations 1 & 2

	Rating	Summary of factors underlying rating
R.1	PC	<ul style="list-style-type: none"> <li>• “Counterfeiting and piracy of products”, and “insider trading and market manipulation” are not predicate offenses to ML.</li> <li>• The ML offense cannot be applied to persons who commit and are convicted</li> </ul>

		<p>for the predicate offense. The inability to do this is not supported by principles that amount to fundamental principles under the FATF standards.</p> <ul style="list-style-type: none"> <li>• Issues of effectiveness: <ul style="list-style-type: none"> <li>○ The comparatively low level of sanctions for the offense and the burden of proof required to establish that proceeds relate to a predicate crime encourage the use of charges other than ML to pursue serious and organized crime or situations of third party ML.</li> <li>○ The restriction on applying the ML offense to persons who are convicted of the predicate offense tends to result in ML investigations being dropped in favor of investigations into the predicate offense.</li> </ul> </li> </ul>
<b>R.2</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Natural and legal persons are not subject to effective, proportionate and dissuasive sanctions for basic ML.</li> <li>• Due to the lack of statistics, assessors could not determine that sanctions are applied effectively to legal persons.</li> </ul>

## 2.2. Criminalization of Terrorist Financing (SR.II)

### 2.2.1. Description and Analysis

#### *Legal Framework:*

202. The financing of terrorist acts and the financing of individual terrorists are criminalized in Germany under Section 89a (2) number 4 of the CC. This provision resulted from the recent amendment to the CC introduced by the Act on the Prosecution of the Preparation of Serious Violent Acts Endangering the State (*Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten, GVVG*) which was passed after the on-site visit and entered into force on August 4, 2009. In addition, according to the authorities, these conducts may be prosecuted based on the participatory offense of “assisting another to commit a crime” pursuant to Section 27 of the CC. The financing of terrorist organizations may be prosecuted based on Section 129a (5) of the CC, which criminalizes the support of terrorist organizations.

203. The financing of terrorist acts and the financing of individual terrorists under Section 89 a (2) number 4 of the CC, and the financing of terrorist organizations under 129a (5) of the CC are predicate offenses to ML.

204. Germany also claims that the financing of terrorist acts and the financing of individual terrorists may be prosecuted based on the participatory offense of “assisting another to commit a crime” (aiding and abetting) pursuant to Section 27 of the CC.

#### *Criminalization of Financing of Terrorism (c. II.1):*

205. The Act on the Prosecution of the Preparation of Serious Violent Acts Endangering the State introduced a new section 89 a (2) number 4 of the CC, thereby criminalizing the collection of assets “not merely insubstantial” in value (*nicht unerhebliche Vermögenswerte*), as well as the conducts of accepting them or making them available, for the preparation of a serious violent act endangering the state.

206. A serious violent act endangering the state is defined as a criminal offense against life within the meaning of Section 211 or 212 of the CC, or against personal freedom within the meaning of Section 239a

or 239b of the CC, which under the circumstances, is intended and apt to interfere with the existence or security of a state or an international organization or to do away with, suspend the application of, or undermine the constitutional principles of the Federal Republic of Germany.

207. Section 89 a (2) number 4 of the CC complements Section 129a of the CC and, in principle, could be interpreted as covering the financing of terrorist acts and individual terrorists. However, a number of shortcomings prevent it from being fully in line with the requirements of SR II.

208. The definition of “serious violent act endangering the state” is not fully consistent with the definition of terrorist act under Article 2 of the Terrorist Financing Convention as it does not extend to all acts that constitute offenses within the scope of, and as defined in the treaties annexed to the Terrorist Financing Convention. A serious violent act endangering the state is also narrower in scope than the generic definition of terrorist act under Article 2 of the Terrorist Financing Convention as it does not cover serious bodily injuries.

209. The term asset under the Act on the Prosecution of the Preparation of Serious Violent Acts Endangering the State is limited by the requirement of having to be “not merely insubstantial.” The *Bundestag* has provided the following reasoning for the term “not merely insubstantial” (as published in the Official Records of the German Parliament (*Bundestagsdrucksache*, BT-Dr) 16/1248 p. 15): “In addition to movable and immovable property of a certain value, the term ‘assets’ (*Vermögenswerte*) covers rights, including claims. Assets that might be deemed insignificant when seen in isolation (‘quantitative assessment’) may be more than merely insubstantial if, in an overall evaluation, they have made a greater than merely insubstantial contribution to the preparation of a serious violent act endangering the state (‘qualitative assessment’). In this context, the perpetrator need not know as a certain fact that the financial support provided constitutes a not merely insignificant contribution to a serious violent act endangering the state, nor does this need to be the perpetrator’s primary objective. Rather, it suffices in this regard for the perpetrator to accept this as being possible and to condone it.”

210. By contrast, SR II does not impose a requirement for the funds to be of a certain minimum value. It broadly requires them to be assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travelers checks, bank checks, money orders, shares, securities, bonds, drafts or letters of credit, whether from a legitimate or illegitimate source. As a result, while the practical impact of this deficiency may be low, the Act on the Prosecution of Serious Violent Acts Endangering the State is not in line with the requirements of SR II on this point either.

211. Section 89a (2) number 4 of the CC does not require the actual act endangering the state to be committed or attempted, nor the funds to be linked to a specific act.

212. In addition to Section 89a (2) number 4, the authorities claim that the financing of terrorist acts and the financing of individual terrorists may also be prosecuted based on the participatory offense of “assisting another to commit a crime” pursuant to Section 27 of the CC. The authorities also argue that, depending on the principal criminal act that the accessory has aided and abetted, the participatory offense pursuant to Section 27 CC may also be a predicate offense to ML.

213. The financing of terrorist organizations is criminalized by Section 129a (5) of the CC.

214. Section 129a (5) of the CC provides that “*anybody who supports [a terrorist organization] may be sanctioned with imprisonment of six months to ten years [if in relation to an organization pursuant to*



*Section 129a (1) and (2)] or of up to five years or a fine [if in relation to an organization pursuant to Section 129a (3)].”*

215. Terrorist organizations pursuant to Section 129a (1) of the CC are those whose purpose it is or whose activities are aimed at committing the offenses of murder (Section 211), manslaughter (Section 212), genocide (Section 6 of the Code of Crimes against International Law), crimes against humanity (Section 7 of the Code of Crimes against International Law), war crimes (Sections 8, 9, 10, 11 or 12 of the Code of Crimes against International Law), or crimes against personal liberty pursuant to Sections 239a or 239b of the CC.

216. In comparison, terrorist organizations pursuant to Section 129a(2) of the CC are those whose purpose it is or whose activities are aimed at:

- causing serious physical or psychological harm to another person, especially in the way described in Section 226;
- committing crimes under Sections 303b (computer sabotage), 305 (destruction of structures), 305a (destruction of important means of work) or crimes dangerous to the general public in cases under Sections 306 to 306c (arson) or Section 307 subsections (1) to (3) (causing an explosion by nuclear power), Section 308 subsections (1) to (4) (causing an explosion by use of explosives), Section 309 subsections (1) to (5) (misuse of ionizing radiation), Sections 313 (causing a flood), 314 (poisoning dangerous to the public) or Section 315 subsections (1), (3) or (4) (dangerous interference with rail ship or air traffic), Section 316b subsection (1) or (3) (interference with public operations) or Section 316c subsections (1) to (3) (assaults on air and sea traffic) or Section 317 subsection (1) (interference with telecommunications facilities);
- Committing crimes against the environment in cases under Section 330a subsections (1) to (3);
- Committing crimes under the Act on Control of Weapons of War, sections 19(1)-(3), 20(1), 20(2), 20a(1)-(3), in each case also in conjunction with section 21, or 22a(1)-(3); or
- Committing crimes under section 51 subsections (1) to (3) of the Weapons Act.

If one of those acts is intended to intimidate seriously the population, to unlawfully coerce a public authority or an international organization through the use of force or the threat of use of force, or to significantly impair or destroy the fundamental political, constitutional, economic or social structures of a country or an international organization, and which, given the nature or consequences of such acts, may seriously damage a country or an international organization.

217. Finally, terrorist organizations pursuant to Section 129a (3) are those whose “aims or activities of the group are directed towards the threatening with the commission of one of the crimes referred to in subsection (1) or (2).”

218. The term “organization” is not defined in the law. However, as mentioned in the analysis of Recommendation 1, a “group” within the meaning of Sections 129 et seq. is deemed to be an organizational combination of at least three persons, designed to exist for a certain period of time, where – with subordination of the will of the individual to the will of the group as a whole — the members pursue common goals, while standing in such relation to one another that they feel themselves to be a uniform cluster.



219. Based on this interpretation, Section 129a is broad enough to cover the commission or attempt, participation as an accomplice, organization or direction of others. However, the term only applies to organizations aimed at carrying out a limited list of offenses. In comparison, the generic offense of Article 2 of the TF Convention is defined to include any act carried out with the required intent. Furthermore, Sections 129 a (1) and (2) of the CC do not extend to all convention offenses as provided for in Article 2 TF Convention. In particular, offenses defined in the Fixed Platform Convention (Article 2(1)(a) and (d)) and the Airport Protocol (Article II (1)(b)) are not covered.

220. For these reasons, the definition of “terrorist organization” pursuant to Section 129a of the CC is not fully in line with the FATF 40+9 Recommendations. However, organizations aimed at carrying out a criminal act not covered by Section 129a CC are nevertheless criminalized under Section 129 CC, which sanctions the support of an organization, the objectives or activities of which are directed towards the commission of offenses in general. The only practical difference between sections 129 CC and 129aCC is the range of sanctions; the sanction for supporting a criminal organization under Section 129 ranges from imprisonment of not more than five years to a fine. Assessors consider this practical difference to have a minor implication.

221. From the language of Section 129a (5), the mere act of supporting a terrorist group constitutes a criminal offense and that it is not required that the support provided to a terrorist organization is actually used to carry out or attempt a specific terrorist act, or that the support is linked to a specific terrorist act.

222. Pursuant to Section 129a (5), whoever supports a group as described in subsection (1), (2) or (3) shall be punished by imprisonment from six months to ten years in cases under subsections (1) and (2), and by imprisonment of up to five years or a fine in cases under subsection (3). Whoever recruits members or supporters for a group as described in subsection (1) or subsection (2) shall be punished by imprisonment from six months to five years.

223. The provision does not define the meaning of the term “support”. However, the authorities claim that, according to the Federal High Court, “the support of a terrorist group” in accordance with Section 129a(5) of the CC, comprises any objectively useful, supportive act, and therefore also all types of provision of funding referred to under the TF Convention.<sup>36</sup> In addition, the authorities provided case law to support their argument that the “collection” of funds to finance terrorist organizations constitutes an offense according to Section 129a of the CC. The mere collection of funds for a terrorist organization is regarded as support of a terrorist organization within the sense of Section 129a (5) of the CC and it is not necessary for the financial means to be used to commit a terrorist act, or for an attempt at such an act. The collection or provision of the funds must simply serve an objective purpose for the terrorist organization and must be useful for it.<sup>37</sup>

224. The financing of a terrorist act or of an individual terrorist under Section 89a of the CC and the financing of a terrorist organization under Section 129a (5) of the CC are less serious offenses (*Vergehen*). Thus, an attempt thereof is only criminal if expressly provided for in the law. In the absence of provisions to that effect, the attempt to finance a terrorist act or an individual terrorist and the attempt to support a terrorist organization are therefore not offences under German law. However, the authorities have explained that, in light of the broad interpretation given to the term “support”, as described above, the

<sup>36</sup> Judgment of October 30, 1964 handed down by the Federal Court of Justice (reference Nbr. 3StR 42-64; and Judgment of October 3, 1979 handed down by the Federal Court of Justice (reference Nbr. 3StR 264-79).

<sup>37</sup> Judgment of December 5, 2007 handed down by the Düsseldorf Higher Regional Court—reference no. III-VI 10/05 2 StE 6/05-8; and Judgment handed down by the Higher Regional Court of Stuttgart on July 15, 2008 (reference no. 5-2 StE 2/05).

terrorist financing offense under 129a (5) would cover any conduct that otherwise would be considered as attempt (*Vorverlagerung der Strafbarkeit*). With respect to section 89a CC, the authorities have explained that since the terms “collecting”, “accepting” or “making available” are even broader than “support”, this offense would also cover any conduct that would otherwise be considered as attempt. As a result, the fact that the attempt to commit these offenses is not criminalized explicitly, as such, has no practical implications.

225. However, criminal liability for “incitement” to finance a terrorist act or an individual terrorist, or to support a terrorist organization and for “assisting” in financing a terrorist act or and individual terrorist, or in supporting a terrorist organization would be criminalized pursuant to Sections 26 and 27 in combination with Sections 89a or 129a (5) of the CC.

226. Notwithstanding the absence of a definition of the term “funds” under Section 129a (5) of the CC, the authorities have provided case law confirming that the “support” of terrorist groups under such section would extend to “any funds” as this term is defined in the TF Convention, whether from a legitimate or illegitimate source.

***Predicate offense for Money Laundering (c. II.2):***

227. The financing of terrorist acts and the financing of individual terrorists criminalized under section 89a (2) number 4 of the CC are both predicate offenses to ML, as they have been listed among those offenses that constitute predicate offenses to ML under section 261 (1) second sentence, number 5 of the CC. In addition, the authorities claim that, depending on the principal criminal act that the accessory has aided and abetted, the participatory offense pursuant to Section 27 CC may also be a predicate offense to ML.

228. The “support of a terrorist organization” is a less serious offense (*Vergehen*) specifically listed in Section 261 (1) second sentence, number (5) of the CC and therefore also qualifies as a predicate offense for ML.

***Jurisdiction for Terrorist Financing offense (c. II.3):***

229. Section 3 of the CC provides that Germany’s criminal laws are applicable to all acts committed in Germany. Section 4 further provides that Germany’s criminal laws also apply to all acts on a vessel or aircraft of Germany, regardless of where the vessel or aircraft was located at the time of the commission of the act.

230. With respect to terrorism financing offenses committed outside Germany, Section 7 of the CC provides that the German CC applies to all acts (1) committed by German citizens or (2) by non-German citizens located in Germany and whose extradition has been either declined or has not been sought. In both cases, the act is only considered to fall under the German CC if the act is criminalized in the country where it occurred. Thus, absent dual criminality, there is no extra-territorial jurisdiction over terrorism financing offenses committed in another country by German citizens, or persons resident in Germany. Section 9 of the CC further provides that an act is considered committed wherever the perpetrator acted or in the case of an omission should have acted or wherever the result of the criminal act occurs or should have occurred.

231. Section 129b of the CC further provides that the offense of “supporting terrorist organizations” pursuant to section 129a is also an offense if the support relates to a foreign terrorist organization. However, with respect to organizations outside the EU, the offense only applies if (1) it was committed through an act exercised within the territorial scope of the CC as outlined above or (2) or the perpetrator is

a German national or located in Germany. In the second case, however, the offense may only be prosecuted subject to approval by the German Ministry of Justice.

***The Mental Element of the TF offense (applying c. 2.2 in R.2):***

232. Pursuant to Section 15 of the CC, only “intentional” acts are considered crimes under German law unless a specific provision expressly criminalizes negligence. Section 129a (5) does not criminalize the negligent support of terrorist groups. Accordingly, only the intentional support of terrorist groups would amount to a criminal offense in Germany under section 129 (5).

233. The authorities have explained that a person may be held criminally liable as a supporter of a terrorist group under Section 129a (5) of the CC if that person had the intention that the funds be used to support a group whose aims or activities were directed towards the commission of the acts referred to under 129a (1) and (2).

234. As explained in the write up for Recommendation 1, Section 261 of the CPC establishes the principle of free evaluation of evidence. This principle states that the facts and circumstances related with the purpose of the proceeding may be admitted by any means of evidence, except for the exceptions provided for in the laws. A means of evidence is admitted if it refers directly or indirectly to the purpose of the investigation and is useful for revealing the truth. Accordingly, the mental element of the TF offense may be inferred through indicia, constituted by external facts and circumstances that are proved in the proceedings

***Liability of Legal Persons (applying c. 2.3 & c. 2.4 in R.2):***

235. German law does not provide for criminal liability of legal persons but regulatory sanctions are available. The detailed analysis outlined under Recommendation 2, elements 2 and 3 also applies to the terrorism financing offense.

***Sanctions for TF (applying c. 2.5 in R.2):***

236. The financing of a terrorist act and the financing of an individual terrorist are sanctioned by imprisonment of six months to ten years under Section 89a (2) (4) of the CC.

237. The support of terrorist groups whose aims or activities are directed to the commission of the crimes referred under Section 129a (1) and (2) is sanctioned by imprisonment from six months to ten years, whereas the support of terrorist groups whose aims or activities are directed towards the threatening of the commission of one of the crimes referred to under Section 129a (1) or (2) is sanctioned by imprisonment of up to five years or a fine.

238. As in the case of the ML offense, TF offenses (including the financing of terrorist acts, the financing of an individual terrorist and the support of terrorist groups) are criminalized in Germany as less serious crimes (*Vergehen*).

239. Given the recent passage of the Act on the Prosecution of the Preparation of Serious Violent Acts Endangering the State (*Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten*, GVVG), there have been no sanctions imposed in Germany for the financing of a terrorist act and the financing of an individual terrorist. As a result, it was not possible to assess the effectiveness of the sanctions for these offenses relative to the penalties actually imposed by the courts.

240. While Germany provided evidence of cases showing that sanctions have been applied for the support of terrorist groups under Section 129a (5) of the CC, no statistics were provided to show the

amount of investigations, prosecutions and convictions, nor the sanctions actually imposed by the courts in relation to this specific offense. The authorities explained that it was not possible to break down the statistics to distinguish the figures related with the support of terrorist groups under 129a (5) of the CC from other broader terrorist offenses under Section 129a of the CC. As a result, it was not possible to fully assess the effectiveness of these sanctions.

241. In addition, Germany has not provided any statistics on the application of administrative fines to legal persons as a result of the commission of TF offenses.

242. Based on the above, assessors were unable to fully assess whether TF offenses in Germany are subject to effective, proportionate and dissuasive sanctions.

**Statistics (R.32):**

243. It should be noted that, due to the recent passage of the Act on the Prosecution of the Preparation of Serious Violent Acts Endangering the State (*Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten, GVVG*), there have been no sanctions imposed in Germany for the financing of a terrorist act and the financing of an individual terrorist. As a result, no statistics are available with regards to offenses under Section 89a (2) (4) of the CC. In addition, the statistics below do not discriminate between the formation of a terrorist group under Section 129a and the specific financing of a terrorist group under Section 129a (5). As a result, no specific statistics are available with regards to the offense under Section 129a (5) CC either.

**Statistical Table 16. Investigations Conducted for Combating Terrorism (including financial investigations)**

	2004	2005	2006	2007
Total	55	52	59	108
Of which based on STRs	16	15	17	16

**Charges and Convictions for Terrorist Offenses**

	2004	2005	2006	2007	2008
Charges: Section 129a (Formation of Terrorist Groups)	2	7	13	4	5
Charges: Section 129b (Formation of Terrorist Groups Abroad)	0	0	0	0	1
Convictions: Section 129a (Formation of Terrorist Groups) - resulting in imprisonment	2 1	7 7	13 13	4 4	5 5
Convictions: Section 129b (Formation of Terrorist Groups Abroad)	0	0	0	0	1

**Convictions for offenses pursuant to Section 129a of the Criminal Code (*Strafgesetzbuch*, StGB)**

Year	Total convictions	Imprisonment or youth custody of more than ... up to (and including) ...						
		9 months–1 year		1–2 year(s)		2–3 years	3–5 years	5–10 years
		without	with	without	with			
		suspension of the sentence		suspension of the sentence				
2003	5			1	2	1	1	
2004	2		1				1	
2005	7				1	2	2	2
2006	13				2	5	2	4
2007	4				2	1		1
2008	5			1		1	1	2

Source: Federal Statistical Office (*Statistisches Bundesamt*) (ed.), *Strafverfolgung* (Prosecution). The figures for the years until 2006 refer to the so-called “old” *Länder*, in other words the Federal Republic of Germany prior to re-unification, including greater Berlin. From 2007, the figures represent all of Germany.

244. The table below shows the number of preliminary criminal investigations and criminal procedures for Section 129a CC offenses where the TF conduct of supporting a terrorist group under Section 129a(5) CC was taken into consideration. It should be noted, however, that, in all of these cases, the focus of the prosecutor was placed on proving whether the TF conduct could amount to “participation in a terrorist group.” The authorities asserted that some of the convictions for Section 129a offenses (*i.e.* convictions for the “participation in” a terrorist group) involved TF conducts.

**Preliminary criminal investigations and criminal procedures for 129a CC Offenses (where the TF conduct of supporting a terrorist group was considered to be “participation in” a terrorist group)**

Year	Number of preliminary criminal investigations in which TF was considered	Number of criminal procedures in which TF was considered
2002	40	1
2003	22	7
2004	20	3
2005	17	2
2006	21	2
2007	20	5
2008	17	6
2009	10	4

***Assessment of Effectiveness***

245. Germany considers radical Islamic terrorism as its primary security threat and claims that it has taken extensive domestic measures against such terrorism since September 11, 2001.

246. However, the categorization of TF offenses as “less serious offenses” is not consistent with the overall priority that Germany assigns to the fight against terrorism. As in the case of the ML offense, it would appear that such categorization could prevent Germany from applying effective, proportional, and

dissuasive sanctions to TF offenders. Once again, in addition to sending a weak message on the relevance that German criminal law assigns to this offense, it generally offers prosecutors and judges a weak range of sanctions to apply as a punishment for the commission of the TF conduct. Moreover, it opens the path to the suspension of the execution of the punishment and the benefit of probation to TF offenders.

247. The recent criminalization of the financing of an individual terrorist and the financing of terrorist acts (under Section 89a (2) (4) CC) means that there are no cases in relation to these offenses yet. The authorities were unable to provide clear and complete statistics on the amount of investigations, prosecutions and convictions for offenses related with the support of terrorist groups (under Section 129a (5) CC). However, as noted above, the authorities explained that some cases where convictions were obtained for participating in terrorist groups (under Section 129a CC) involved TF conducts.

248. The lack of clear and complete statistics regarding the implementation of the TF offenses means that the assessors were unable to fully assess their effective implementation. The technical deficiencies in the TF offense and its inconsistencies with the TF Convention may be limiting Germany's capacity to prosecute and convict TF offenders effectively and may theoretically prevent Germany from providing certain forms of international cooperation where dual criminality is required (*i.e.* extradition with non-EU jurisdictions).

249. The absence of criminal liability for legal persons and the lack of administrative fines effectively applied to legal persons do not seem to constitute a strong deterrent to the unlawful use of legal persons by terrorist financiers either.

### 2.2.2. Recommendations and Comments

250. In order to comply fully with Special Recommendation II Germany should:

- Criminalize the financing of a terrorist act and of an individual terrorist consistent with Article 2 of the TF Convention.
- Undertake actions (awareness raising or training) to increase the application of regulatory sanctions against legal persons.
- Increase the minimum range of sanctions applicable to TF so that it is made a serious offense.
- Maintain complete statistics on the amount of investigations, prosecutions, and convictions for TF offenses.

### 2.2.3. Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	LC	<ul style="list-style-type: none"> <li>• The definition of "serious violent act endangering the state" is not fully consistent with SR II as it does not extend to all acts that constitute offenses within the scope of, and as defined in the treaties annexed to, the Terrorist Financing Convention and it does not cover serious bodily injuries.</li> <li>• The definition of the term "funds" in connection with the financing of a terrorist act or individual terrorist is not fully in line with the requirements of SR II, as it imposes a requirement for the funds to be of a certain minimum value (<i>i.e.</i> not merely insubstantial).</li> <li>• The minimum level of sanctions raises the possibility that the sanctions</li> </ul>

	Rating	Summary of factors underlying rating
		<p>imposed may not be effective, proportionate and dissuasive.</p> <ul style="list-style-type: none"> <li>Effectiveness not established due to the lack of specific statistics.</li> </ul>

## 2.3. Confiscation, freezing and seizing of proceeds of crime (R.3)

### 2.3.1. Description and Analysis

#### *Legal Framework:*

251. Title VII of the German CC is entitled “Forfeiture and Confiscation.” This Title contains one provision dealing with the forfeiture of assets (Section 73), mainly used for proceeds, and another one dealing with confiscation of assets, (Section 74), mainly used for instrumentalities. Note that forfeiture and confiscation, in practice, result in the same outcome. However, while forfeiture pursuant to Section 73 of the CC is a mandatory based sanction, confiscation pursuant to Section 74 is a measure that may be taken, subject to the court’s discretion.

252. Both provisions apply to all offenses in the German CC. This includes to all predicate offenses for ML as well as the ML offenses in Section 261 of the CC and terrorism financing offenses pursuant to Sections 89a and 129a (5) of the CC. In addition, both provisions also apply where the offense of “supporting a terrorist organization” is committed with respect to a foreign terrorist organization within the scope of Section 129b of the CC.

253. As a general rule, both Sections 73 and 74 of the CC may be invoked only on the basis of a conviction for the underlying criminal offense. In certain circumstances, however, and subject to the requirements under these same Section, Section 76a of the CC allows for the issuance of an independent confiscation order even in cases where for factual reasons no specific person can be prosecuted or convicted (i.e., when the person cannot be found). Such orders may not, however, be issued in the absence of a complaint, request for prosecution or authorization.

254. Provisional measures with respect to property that may become subject to confiscation are provided for in Section 111b to 111l of the CPC.

#### *Confiscation of Property related to ML, TF or other predicate offenses including property of corresponding value (c. 3.1);*

#### **Proceeds**

255. Section 73 provides the legal basis for the forfeiture of proceeds obtained from the commission of any predicate, ML or terrorism financing offense. As a mandatory sanction, when an offense has been committed the court shall order forfeiture (*Verfall*) of the property which constitutes proceeds from such offense.

256. Section 73 of the CC provides that forfeiture can also extend to all “benefits derived from” such proceeds, including indirect proceeds (i.e. objects obtained through alienation of the items obtained through the commission of a crime, objects obtained as a replacement for the destruction, damaging or withdrawal of an item obtained through the commission of an offense, or objects obtained on the basis of an acquired right, such as a claim that the perpetrator may have against someone).



257. If the perpetrator or accessory acted on behalf of another person and that person obtained a benefit, the forfeiture may be directed against that person. The forfeiture may also be directed against property owned by a third party if the third party furnished the property for the commission of the criminal act or with knowledge of the attendant circumstances of the act.

258. Section 73d of the CC also provides for an “extended forfeiture” by setting forth that “If an unlawful act has been committed pursuant to a law which refers to this provision, then the court shall also order the forfeiture of objects of the perpetrator or inciter or accessory if the circumstances justify the assumption that these objects were acquired as a result of unlawful acts, or for the purpose of committing them. This shall also be applicable if the perpetrator or inciter or accessory does not own or have a claim to the object only because he acquired the object as a result of an unlawful act or for the purpose of committing it.”

259. Pursuant to the ML offense under Section 261 (7) the extended forfeiture under Section 73d “shall be applied to any perpetrator acting to make a profit or as a member of a gang formed for the purpose of repeatedly committing such offenses.”

### **Instrumentalities**

260. Section 74 of the CC expressly allows for the “confiscation” of any instrumentalities used or intended for use in the commission of any intentional criminal offense if they are owned by the perpetrator or accessory or are dangerous or may be used to commit another criminal offense.

261. In general, confiscation of instrumentalities held or owned by third parties is possible in very limited circumstances (*i.e.* when they are dangerous or may be used to commit another criminal offense).

262. However, Section 74a of the CC provides that even where property owned by a third party is not dangerous or may be used in the commission of another offense, it may be confiscated if the person who owns it (1) has at least recklessly contributed to the fact that the property or the right thereto has been the object of the criminal act or its preparation or (2) has acquired the objects in a reprehensible manner with knowledge of the circumstances which would have permitted their confiscation. In all other situations, Section 74 of the CC does not provide for the confiscation of instrumentalities owned by third parties (whether they are held by the defendant or the third party).

### **Equivalent Value Confiscation**

263. German law contains a series of provisions dealing with the forfeiture and confiscation of property of corresponding value. If forfeiture of a particular property is not possible, the court shall order forfeiture of a sum of money equivalent in value to the property in question. The same applies with regard to property which would be subject to confiscation.

264. Section 73a of the CC allows for the forfeiture of a sum of money in an amount equivalent to the proceeds of crime in cases where (1) the forfeiture of a specific object is impossible due to the nature of the object or for some other reason or (2) if the value of the object is less than the value of the object originally acquired.

265. Section 74c of the CC allows for the confiscation of a sum of money equivalent in value to instrumentalities used or intended for use in the commission of an intentional crime if the perpetrator or accessory owned the property at the time of commission of the act but before issuance of the confiscation order uses or alienates the property or otherwise frustrates the confiscation of the property. Furthermore, equivalent value confiscations may be ordered in addition to the confiscation of the property in cases where the perpetrator or accessory, before issuance of the confiscation order, grants a third person a right

with respect to the property and the court cannot order the extinguishment of that right without compensation. However, Section 74c of the CC provides that the court may decide not to order a confiscation if, at the time of the order, the value of the originally acquired proceeds is no longer part of the affected person's assets or the objects acquired are only of slight value, whereby the court is allowed to estimate the value of the property.

***Confiscation of Property Derived from Proceeds of Crime (c. 3.1.1 applying c. 3.1):***

266. Section 73(2) sets forth that forfeitures can be extended to derived benefits and then lists certain indirect proceeds (such as objects which the perpetrator or inciter or accessory has acquired through alienation of an acquired object, as a replacement for its destruction, damage or seizure or on the basis of an acquired right). According to the authorities, the reference to “derived benefits” comprises property that is derived directly or indirectly from proceeds of crime; including income, profits, or other benefits from the proceeds of crime.

267. The terms used in section 73 (2) of the CC (StGB) correspond to the terms defined in the Civil Code (*Bürgerliches Gesetzbuch*, BGB): derived benefits (Section 73(2) first sentence of the CC) are the fruits and emoluments of a thing or right (Section 100 of the Civil Code). Fruits are the products, other yield of the accession and the proceeds (Section 99 of the Civil Code). Indirect proceeds are defined in Section 73 (2) second sentence of the CC as “objects which the perpetrator or inciter or accessory has acquired through alienation of an acquired object” as replacements for an object initially acquired by that person and forming part of his or her assets, regardless of whether such replacement is made by another object or by an acquired right. It is also irrelevant whether or not the indirect proceed has become part of the assets of the perpetrator, inciter or accessory as a legal consequence that was not intended by that person, or that the person could not at all influence, or whether it was the unavoidable consequence of a legal transaction. The intention to prevent the perpetrator, inciter or accessory from benefiting from the replacement of the economic asset gained for the offense or obtained as a result of it. Similarly, it is not just the principal object gained for the offense or obtained as a result of it that is to be taken from the perpetrator, inciter or accessory, but additionally the economic benefits that the principal object has provided to that person. This means that forfeiture is expanded to cover all proceeds gained by criminal offenses.<sup>38</sup>

***Provisional Measures to Prevent Dealing in Property subject to Confiscation (c. 3.2):***

268. Section 111b of the CPC allows for the seizing of moveable as well as immoveable property based on reasonable grounds to suspect that the conditions for the forfeiture or confiscation of such property have been met.

269. Pursuant to Section 111b (2) of the CPC the seizing measures may also extend to property of equivalent value to such moveable or immoveable property if there are reasonable grounds to suspect that the conditions for an equivalent value forfeiture or confiscation have been met.

270. The conditions for forfeiture to be met require an unlawful act to be committed and the perpetrator or inciter or accessory to have acquired something as a result thereof or for the purpose of committing it. The conditions for confiscation to be met require an intentional crime to be committed for

<sup>38</sup>

cf. Fischer, Commentary on the Criminal Code, section 73, marginal number 25 et seq.; ruling published by the Federal Court of Justice (BGH) published in New Judicial Weekly Journal (*Neue Juristische Wochenschrift*, NJW) 1986, p. 1186.

the objects which were generated thereby or used or intended for use in its commission or preparation to be confiscated.

271. Seizures may be directed against any object subject to forfeiture or confiscation, including equivalent value forfeitures and confiscations, with the exception of the following objects, which pursuant to Section 97 (1) of the CPC, shall not be subject to seizure: *i*) written correspondence between the accused and the persons who, according to Section 52 or Section 53 subsection (1), numbers 1 to 3b, may refuse to testify; *ii*) notes made by the persons specified in Section 53 subsection (1), first sentence, numbers 1 to 3b, concerning confidential information entrusted to them by the accused or concerning other circumstances covered by the right of refusal to testify; and *iii*) other objects, including the findings of medical examinations, which are covered by the right of the persons mentioned in Section 53 subsection (1), first sentence, numbers 1 to 3b, to refuse to testify.

272. Pursuant to Section 97 (2) of the CPC the restrictions on seizure referred to in the preceding paragraph shall not apply if certain facts substantiate the suspicion that the person entitled to refuse to testify was involved in the offense, or as inciter or accessory, in obstruction of justice or handling stolen goods, or where the objects concerned have been obtained by means of a criminal offense or have been used or are intended for use in perpetrating a criminal offense, or where they emanate from a criminal offense.

273. As a general rule, Article 111e of the CPC provides that any seizing orders may only be issued by a court. In exigent circumstances, the prosecutor may order the seizing of any property and the investigator may order the seizing of moveable property even in the absence of a court order. If the measure has been ordered by the prosecutor, the court's approval has to be obtained within one week of the taking of the measure. In cases involving moveable property, however, court approval is not required, regardless of whether the measure was ordered by the prosecutor or the investigator. Rather, the person affected by the seizing measure has a right to appeal to the court at any given time with a view to having the measure removed.

274. Seizures may be ordered at any instance of the proceedings, even where no public charges have been preferred, so long as there are reasonable grounds to suspect that the conditions for forfeiture or confiscation of the objects involved have been met.

275. Pursuant to Section 111b (3) of the CPC, any seizing measures have to be lifted by the court after six months if no strong grounds exist. The court may, however, extend the measure for another six months based on an application by the prosecutor if certain facts substantiate the suspicion and if either the criminal investigations are very complicated or very extensive, or if another important reason exists. Absent strong grounds, no seizing measure may be enforced beyond twelve months.

276. Depending on the property affected, Section 111c of the CPC provides that seizing measures are implemented through seal or any other form of mark (for moveable property), through registration in the real estate cadastre (for real estate or land or rights with respect to real estate or land), through attachment (for claims or property rights), or entry into the registry (for ships, ship constructions and aircrafts). Any measures taken to implement a seizing order may be appealed against to the court pursuant to Section 111f (5) of the CPC.

### ***Ex Parte Application for Provisional Measures (c. 3.3 ):***

277. Section 33 of the CPC provides that as a general rule, any person that may be affected by the decision of a court has the right to be heard. Where the decision relates to the seizing of property, however,

Section 33 (4) provides that the measure may be taken *ex parte* if granting the person concerned a hearing would endanger the purpose of the measure.

***Identification and Tracing of Property subject to Confiscation (c. 3.4):***

278. Under German criminal law, confiscation and forfeiture constitute incidental consequences of a criminal act. As a result the entire range of investigative techniques of the CPC is available for investigating the matter to the extent that it also applies to the preconditions of these incidental consequences. Thus, the criminal investigation authorities have a comprehensive repertoire of investigative techniques at their disposal for ascertaining the origin and ownership of property that could be subject to confiscation or forfeiture, including the following: requests for information by the public prosecutor's office to other competent authorities (e.g., in order to obtain account records through the BaFin etc., section 161 of the CPC); searches (Sections 102 and 103), usually on the basis of a court order; telephone interceptions (sections 100a *et seq.*), usually on the basis of a court order; questioning witnesses or accused persons (e.g., sections 58 *et seq.*, 133 *et seq.* and 161 *et seq.*); or the use of undercover agents (section 110a *et seq.*), among others.

279. In the case of DNFBPs protected by professional privilege (lawyers, and notaries, auditors and tax advisors), the conditions restricting access to information, discussed under the DNFBPs section, (in particular the very broad interpretation of what constitutes “legal advice,” also discussed in that section) may substantially limit the right of law enforcement agencies to obtain information and to identify and trace property that is or may become subject to forfeiture/confiscation or is suspected of being the proceeds of crime.

***Protection of Bona Fide Third Parties (c. 3.5):***

280. In the situation of provisional measures which are ordered by the criminal prosecutor (e.g. seizure of objects) the person concerned has always the right to apply for judicial decision at any time (Section 111e(2), Cl. 3 of the CPC). The public prosecution office shall inform the person who is aggrieved as a result of the act without delay of enforcement of the order for seizure or attachment, insofar as that person's identity is known or becomes known during the course of proceedings. Section 111f subsection states that the person concerned may at any time apply for a judicial decision in respect of measures taken in the course of enforcing the seizure or attachment. Against orders of the judge in preliminary proceedings a complaint can be brought (Section 304(1) of the CPC). The right for a complaint also exists for an owner of property who is actually not in possession of it if that owner's right to reclaim for return is endangered by the measure. If the provisional measures has the nature of an attachment *in rem* (*dinglicher Arrest*), Section 111 d states that sections 917 and 920 subsection (1) as well as sections 923, 928, 930 to 932, and 934 subsection (1) of the Civil Procedure Code shall apply *mutatis mutandis*.

281. In addition, the rights of bona fide third parties are protected from any forfeiture and confiscation measures pursuant to Sections 73e and 74e of the CC, respectively. According to these provisions, the rights of third parties remain unaffected by the transfer of title to the state subsequent to the confiscation of the property. Accordingly, bona fide third parties may claim their rights with respect to the confiscated property against the state.

282. For forfeiture pursuant to Section 73 of the CC, the court may never declare the rights of third parties with respect to the forfeited property extinct.

283. For property confiscated pursuant to Section 74 of the CC the court has to order the rights of third parties to be extinct if (a) the object to be confiscated is dangerous or may be used in the commission of another offense pursuant to Section 74(2) or (b) the third party is not bona fide (the party has at least

recklessly contributed to the fact that the property or the right thereto has been the object of the criminal act or its preparation or has acquired the objects in a reprehensible manner with knowledge of the circumstances which would have permitted their confiscation or destruction). If the court extinguishes the rights of third parties for confiscated property that is dangerous or may be used in the commission of another offense, compensation pursuant to Section 74f of the CC and based on fair market value has to be paid.

***Power to Void Actions (c. 3.6):***

284. Sections 134 and 138(1) of the Civil Procedure Code contain authority to take steps to prevent or void actions, whether contractual or otherwise, where the persons involved knew or should have known that as a result of those actions the authorities would be prejudiced in their ability to recover property subject to forfeiture or confiscation.

***Statistics (R.32): Property Seized and Forfeited 2004-2007***

285. The annual asset confiscation statistics reveal the following for the years 2004–2007: In the annual asset confiscation statistics, the data on frozen and seized assets is for the most part recorded from the “police perspective” *i.e.* it reflects statistics on information received.

Statistical Table 17: Total Assets Forfeited and Confiscated 2004-2007

	2004	2005	2006	2007	Total (or average)	(USD)
Number of supported proceedings	6 045	6 010	6 101	7 050	25 206	n.a.
Total (state and civil) claim derived from the crime	EUR 1 268 199 663	EUR 1 191 177 478	EUR 1 066 424 021	EUR 591 737 295	EUR 4 117 538 457	USD 5 730 378 271
Average amount claimed per proceeding	EUR 209 793	EUR 198 199	EUR 174 795	EUR 83 934	EUR 163 355	USD 227 341
Forfeited assets derived from the crime (73ff PC)	N/A	EUR 255 455 658	EUR 284 351 307	EUR 200 145 006	EUR 739 951 971	USD 1 029 791 158
Average amount forfeited	N/A	EUR 42 505	EUR 46 607	EUR 28 389	EUR 29 356	USD 40 855
Confiscated instruments of crime (74ff PC)	N/A	EUR 63 467 338	EUR 15 347 298	EUR 16 869 508	EUR 95 684 144	USD 133 163 623
Other	N/A	EUR 359,159	EUR 871.913	EUR 1 768 055	EUR 2,999,127	USD 4 173 885
Total assets forfeited/ confiscated	EUR 305 963 158	EUR 319 282 155	EUR 300 570 519	EUR 218 782 569	EUR 1 144 598 401	USD 1 592 937 595
USD	USD 425 808 927	USD 444 344 975	USD 418 303 991	USD 304 479 701	USD 1 592 937 595	n.a.
Average amount forfeited or confiscated per proceeding	EUR 50 614	EUR 53 125	EUR 49 266	EUR 31 033	EUR 45 410	USD 63 197
USD	USD 70 440	USD 73 934	USD 68 563	USD 43 189	USD 63 197	n.a.
Total assets forfeited or confiscated as percentage of total claim	24.1%	26.8%	28.2%	37.0%	27.8%	n.a.

**Statistical Table 18: Total Assets Forfeited or Confiscated in Relation to Single Offenses**

<b>Offense</b>	<b>2004</b>	<b>2005</b>	<b>2006</b>	<b>2007</b>
Offenses under the Pharmaceutical Products Act ( <i>Arzneimittelgesetz</i> )	EUR 803 526	EUR 1 567 886	EUR 4 485 342	EUR 1 561 923
Exploiting prostitutes	EUR 223 052	EUR 292 503	EUR 137 209	EUR 128 773
Offenses under the Residence Act ( <i>Aufenthaltsgesetz</i> )				EUR 125 949
Offenses under the Foreigners' Act ( <i>Ausländergesetz</i> )		EUR 2 178 200	EUR 1 167 217	
Offenses under the Foreign Trade and Payments Act ( <i>Außenwirtschaftsgesetz</i> )	EUR 438 030	EUR 2 397 648	EUR 2 935,609	EUR 995 326
Fraud	EUR 83 718 721	EUR 94 069 333	EUR 90 905 548	EUR 42 407 770
Offenses under the Narcotics Act ( <i>Betäubungsmittelgesetz</i> )	EUR 24 960 526	EUR 24 502 310	EUR 17 965 918	EUR 26 605 233
Theft	EUR 14 157 306	EUR 22 352 451	EUR 21 314 250	EUR 10 623 526
Extortion	EUR 1 718 896	EUR 1 470 868	EUR 3 212 876	EUR 816 438
Counterfeiting currency	EUR 112 217	EUR 76 748	EUR 122 103	EUR 115 690
Money laundering	EUR 32 948 160	EUR 65 453 313	EUR 23 710 160	EUR 15 074 378
Receiving stolen goods	EUR 8 473 818	EUR 7 649 729	EUR 4 807 081	EUR 13 123 400
Insolvency offenses	EUR 806,554	EUR 2 145 256	EUR 2 731 136	EUR 1 401,939
Corruption	EUR 7 277 041	EUR 12 946 661	EUR 12 303 645	EUR 2 900 715
Offenses under the War Weapons Control Act ( <i>Kriegswaffenkontrollgesetz</i> )	EUR 152 082	EUR 5 221 800	EUR 0	EUR 427 583
Offenses under the Food and Consumer Goods Act ( <i>Lebensmittelgesetz</i> )	EUR 25 953	EUR 507 762	EUR 423 222	EUR 0
Human trafficking	EUR 2 973 397	EUR 1 298 791	EUR 429 798	EUR 3 200,287
Offenses under the OwiG	EUR 86 568	EUR 390 535	EUR 470 372	EUR 524 071
Police law	EUR 332 184	EUR 162 460	EUR 609 902	EUR 1 314 191
Robbery	EUR 4 327 930	EUR 3 069 560	EUR 2 969 293	EUR 1 106 286
State security offenses	EUR 1 679 109	EUR 55 045	EUR 1 912 564	EUR 2 500
Tax offenses	EUR 12 664 124	EUR 22 211 136	EUR 25 326 589	EUR 6, 360 522
Homicide	EUR 97 431	EUR 338 280	EUR 5 978	EUR 117 568
Environmental crimes	EUR 474 168	EUR 2 121 215	EUR 982 961	EUR 2 169 474
Unfair competition		EUR 3 954 449	EUR 24,230	EUR 104,192
Unlawful gambling	EUR 5 648 747	EUR 2 785 632	EUR 2 323 197	EUR 4 167 775
Misappropriation	EUR 2 790 641	EUR 6 951 645	EUR 5 088 449	EUR 6 347 346
Breach of fiduciary duty	EUR 32 055 691	EUR 23 003 287	EUR 66 641 341	EUR 30 528 553
Offenses under the Copyright Act		EUR 383 031	EUR 1 261 371	EUR 888 702



Offense	2004	2005	2006	2007
<i>(Urheberrechtsgesetz)</i>				
Offenses relating to the falsification of documents	EUR 2 975 457	EUR 1 411 248	EUR 22 495	EUR 3 124 135
Distributing pornographic material	EUR 191 220	EUR 277 728	EUR 264 915	EUR 351 460
Offenses under the VereinsG		EUR 2 148	EUR 511 995	EUR 0
Offenses relating to securities		EUR 230 117	EUR 270 517	EUR 39 768 748
Offenses under the Weapons Act ( <i>Waffengesetz</i> )	EUR 403 890	EUR 196 834	EUR 15 240	EUR 128 943
Procuration	EUR 787 969	EUR 1 042 498	EUR 34 318	EUR 111 319
Other	EUR 18 139 872	EUR 6 564 049	EUR 5 183 677	EUR 2 157 854
<b>TOTAL:</b>	<b>EUR 305 963 158</b>	<b>EUR 319 282 155</b>	<b>EUR 300 570 519</b>	<b>EUR 218 782 569</b>
<b>USD</b>	<b>USD 425 808 927</b>	<b>USD 444 344 975</b>	<b>USD 418 303 991</b>	<b>USD 304 479 701</b>

**Statistical Table 19. Selected Comparative Information for Assets frozen, restrained, seized, forfeited or confiscated taken from 15 Mutual Evaluation or Detailed Assessment Reports for countries evaluated as LC or higher under the FATF 2004 Methodology**

Indicator	Comparative Group Average <sup>39</sup>	Germany (2004-2007 <sup>40</sup> )
Assets frozen, restrained or seized		
Total latest 4 years	USD 246 million	Not Available
Annual value	USD 104 million	Not Available
Annual value per million of population	USD 1.46	Not Available
Annual value as % of GDP	0.0060%	Not Available
Assets ordered forfeited (or confiscated)		
Total	USD 177 million	USD 5 266 million
Annual Value	USD 70 million	USD 1 316 million
Annual value per million of population	USD 1.11	USD 17.72
Annual value as % of GDP	0.0044%	0.0550%
Annual value compared to annual value assets frozen, restrained or seized	67%	Not Available
Assets forfeited or confiscated		
Total	USD 2,902 million	USD 1 464 million
Annual Value	USD 733 million	USD 366 million
Annual value per million of population	USD 2.94	USD 4.93
Annual value as % of GDP	0.0270%	0.0153%

<sup>39</sup> The countries are: Australia, Canada, Denmark, Ireland, Italy, Japan, Mexico, Norway, Portugal, Russia, Singapore, Spain, Sweden, Thailand, U.K., and U.S.A.

<sup>40</sup> The data for the years prior to 2006 has been analyzed using estimates of population and GDP for those years for pre-unification Germany.

Indicator	Comparative Group Average <sup>39</sup>	Germany (2004-2007 <sup>40</sup> )
Annual value compared to annual value assets frozen, restrained or seized	702%	Not Available
Annual value compared to annual value assets ordered forfeited or confiscated	1045%	28%

286. A preliminary analysis by IMF staff of freezing, seizing, and confiscation data in 15 countries assessed under the FATF 2004 Methodology for which data are available suggests that Germany is more effective at obtaining orders to get assets confiscated than at actually confiscating those assets. Germany has obtained forfeiture and confiscation orders relating to more than USD 5 billion over the last four years – more than any other country in the comparative group. Normalizing this amount for population or GDP still indicates that Germany is the most effective country in the comparative group at obtaining such orders. However, Germany does not actually forfeit or confiscate as many assets as the average of countries in the comparative group. Note that the amount forfeited and confiscated measures favorably when compared to the size of Germany’s population, but is below average when compared to the size of Germany’s GDP.

***Additional Elements (Rec. 3) – Provision for a) Confiscation of assets from organizations principally criminal in nature; b) Civil forfeiture and ; c) Confiscation of Property which Reverses Burden of Proof (c. 3.7):***

287. German law provides for comprehensive means of regulating the forfeiture and confiscation of assets belonging to criminal organizations. The extension of Sections 73d, 74a and 261 of the CC not only refers to terrorist organizations, but also applies to “normal” criminal organizations. As a consequence, this means that, in principle, all “criminal” profits these organizations make, even if individual acts cannot be ascertained, as well as all assets belonging to these organizations and supporting them may be forfeited or confiscated.

288. As a general rule, German law does not provide for the forfeiture or confiscation of property without a conviction of any person (*i.e.* civil forfeiture) nor for the forfeiture/confiscation of property which require an offender to demonstrate the lawful origin of the property. However, as mentioned above, an exception to this rule would be those circumstances where for factual reasons no specific person can be prosecuted or convicted (*i.e.* when the person cannot be found). Such orders may not, however, be issued in the absence of a complaint, request for prosecution, or authorization.

### ***Assessment of Effectiveness***

289. From a formal perspective, Germany has the necessary measures, similar to those set forth in the Vienna and Palermo Conventions, to enable its competent authorities to confiscate property laundered, proceeds from ML or predicate offenses, instrumentalities used in or intended for use in the commission of these offenses, or property of corresponding value, without prejudicing the rights of bona fide third parties.

290. The scope of application of these measures is not confined to the criminal offense of ML or to predicate offenses. Germany permits the forfeiture and confiscation of property that is proceeds from TF, or of property that is used or intended to be used for the commission or preparation of TF.

291. Germany has been applying forfeiture and confiscation provisions in numerous cases concerning a wide range of offenses, including ML offenses, although could actually confiscate and forfeit more assets subject to confiscation and forfeiture orders. However, the statistics presented by the authorities do not allow assessors to distinguish in how many ML cases these provisions have been applied each year, nor how much value corresponds to forfeitures and how much to confiscations in the context of ML cases, nor

what type of assets are being forfeited and confiscated in the context of ML cases. Moreover, since Germany did not provide any figures on the forfeiture and confiscation of property in cases concerning TF, it was not possible to assess whether Germany is in fact forfeiting property in cases concerning TF.

292. Procedural law allows for provisional measures such as the seizing of moveable as well as immovable property to prevent any dealing transfer or disposal of property subject to forfeiture/confiscation. However, Germany did not provide any statistics on the application of provisional measures so it was not possible to assess their effective implementation. Nevertheless, given the high value of forfeitures and confiscations, assessors have no reason to doubt the authorities' claim that provisional measures are being applied in Germany. There is the possibility, however, that the use of provisional measures could be improved to help increase the level of assets confiscated and forfeited compared to the total claim made by the State for confiscation and forfeiture.

293. German law permits the entire range of its authorized investigative techniques to be used by its law enforcement agencies to conduct forfeiture investigations and to identify and trace property. However, in the case of DNFBPs protected by professional privilege (lawyers, and notaries, auditors and tax advisers) the conditions restricting access to information, discussed under the DNFBPs section, (in particular the very broad interpretation of what constitutes "legal advice", also discussed in that section) may substantially limit the right of law enforcement agencies to obtain information and to identify and trace some property.

294. Assessors were not alerted as to any particular obstacles in implementing provisional measures or forfeitures and confiscations. The German authorities indicated that, in practice, the public prosecutor's offices use such means in all proceedings in which it can be assumed that the assets will be identified, frozen, seized and confiscated (*Vermögensabschöpfung*). In this regard, the authorities noted that measures are generally taken as early as possible to seize the assets held by a party charged with a crime, at the beginning of criminal investigation procedures, in order to prevent the assets from being removed illicitly. However, some prosecutors also indicated that seizures were typically used to the extent that they can support the evidence in a criminal investigation and not as means to prevent the dealing, transfer or disposal of property subject to forfeiture or confiscation.

### 2.3.2. Recommendations and Comments

295. In order to comply fully with Recommendation 3, Germany should:

- Enable law enforcement authorities to obtain access to information about ownership of property held by DNFBPs who claim that information is protected by professional secrecy rules.
- Improve performance for actually confiscating or forfeiting assets once courts order those assets be confiscated or forfeited.
- Establish a mechanism to collect and keep statistics on provisional measures applied.

### 2.3.3. Compliance with Recommendation 3

	Rating	Summary of factors underlying rating
R.3	LC	<ul style="list-style-type: none"> <li>Professional secrecy is interpreted broadly by the liberal professions, and there are strict conditions for obtaining or compelling information subject to it, which hinder the possibility for law enforcement authorities to locate and trace property.</li> <li>Assets actually forfeited or confiscated are low compared to the total value of assets subjected to orders for forfeiture or confiscation.</li> </ul>

## 2.4. Freezing of funds used for terrorist financing (SR.III)

### 2.4.1 Description and Analysis

#### Legal Framework:

296. Germany freezes funds and assets used for TF on the basis of EC-regulations and complementary domestic legislation. UN Security Council Resolution 1267 (1999), 1390 (2002), and 1455 (2003) are implemented by Council Regulation No. 881/2002 of May 27, 2002, whereas, the most important part of S/RES 1373/2001, is implemented by Council Regulation No. 2580/2001 of December 27, 2001. The Council Regulations are directly applicable law in Germany. Funds and assets are frozen directly and immediately by the Council Regulations.

297. However, with regards to freezing measures within the competency of the EU (*i.e.* matters covered by EC Regulations), Member States may only adopt preliminary national measures, (*i.e.* the Member States may freeze only as long as the EU has not taken action). In this regard, and as complementary national legislation that is in line with the EC Treaty, Germany has enacted Section 6a of the Banking Act and Sections 7(1) and 2(2) of the Foreign Trade and Payments Act (FTPA).<sup>41</sup>

298. Section 6a of the Banking Act provides the competent authorities with financial sanctions and other administrative measures to freeze the “funds” of EU-internals<sup>42</sup> held in German banks. EU-internals are not covered by Council Regulation No. 2580/01 due to the scope of the EU Common Foreign and Security Policy (no rules on merely internal EU affairs, but only on external relations).

299. This kind of freeze takes place in connection with a criminal investigation opened on the basis of information received from another jurisdiction or as a result of an STR filed in relation to a person not on either of the UN lists. If a founded suspicion arises that funds belong to terrorist organizations, or that funds are used to support a terrorist organization, prosecutors also have a duty to institute criminal proceedings pursuant to Section 129a (5) of the CC and apply for appropriate measures at court (provisional injunctions to freeze property, such as seizure or sequestration).

300. Sections 7(1) and 2(2) of the FTPA jointly enable the competent authorities to take preliminary measures to restrict capital and payment transactions involving persons or organizations in the time

<sup>41</sup> Since Article 56 of the EC Treaty (TEC) prohibits all restrictions on the movement of capital and all restrictions on payments, national legislation imposing such restrictions must fall within the scope of one of the exceptions laid down in the EC Treaty in order to be compatible with European Law. In general, measures to combat terrorist financing would fall under these exceptions.

<sup>42</sup> While there is no definition of EU-externals or EU-internals, the list contained under EC Regulation 2580/2001 implies that the differentiating factor is the main location of the terrorist or terrorist organization.

between the notification of a person or organization to the Al-Qaeda and Taliban Sanctions Committee and the implementation of the decision of that Committee by means of an amendment to EC legislation.

301. In addition to the above mentioned Regulations, the EU adopted two Council Common Positions, No. 2001/930/CFSP and No. 2001/931/CFSP on the fight against terrorism, which are applicable also to persons, groups and entities based or residents within the European Union (referred to herein as EU-residents). The implementation of these measures requires subsequent enactment of national legislation and Germany has not yet issued such implementing legislation. Germany has issued Section 6a of the Banking Act. However, this provision implements these requirements only concerning funds of EU-internals held in German banks.

302. So far, approximately 25 names for a EU-or UN-listing have been put forward by Germany. At the time of the on-site visit, Germany had frozen funds amounting to EUR 8 953.07 (USD 12 460) pursuant to Council Regulation (EC) No. 881/2002 (implements UNSCR 1267), and funds amounting to EUR 203.93 (USD 284) pursuant to Council Regulation (EC) No. 2580/2001 (implements UNSCR 1373). Germany has argued that no assets are frozen in Germany as the designated persons, groups and entities have no assets there.

***Freezing Assets under S/Res/1267 (c. III.1):***

303. Germany's framework for implementation of the financing of terrorism aspects of UNSCR 1267 and subsequent resolutions in the sanctions regime against Al Qaida or the Taliban is through EC Regulation 881/2002. Under general European law principles EC Regulation 881/2002 serves as statutory law in Germany. Under the regulation, all funds and economic resources belonging to, or owned or held by a natural or legal person, group or entity designated by the EU Sanctions Committee and listed in the annex of the regulation are frozen. The list under EC Regulation 881/2002 contains both EU-externals and EU-internals. Funds are frozen directly and immediately by the Council Regulation on the day the regulation or and amendments to it enter into force.

304. The assets subject to freezing are defined in very broad terms by EC Regulation 881/2002 (for they include funds, other financial assets and economic resources); these assets are those belonging to, or owned or held by the designated persons or entities – however acquired. The language covers funds or other assets that are either directly or indirectly owned or controlled.

305. The European Commission updates Regulation 881/2002 within three working days, if possible, of any change being made to the UN list. Council Regulation No. 881/2002 has been amended 110 times since its entry into force.

306. In order to fill the gap between the notification of a person or organization to the Sanctions Committee and the implementation of the decision of the Sanctions Committee by means of an amendment to EC Council Regulation No. 881/2002, competent authorities can take preliminary national measures to restrict capital and payment transactions. Sections 7(1) 2(2) of the FTPA serves this purpose. Such national freezing orders prevent the targeted persons or entities from withdrawing their financial assets before entry into force of the Community legislation implementing the decisions of the Security Council Committee.

***Freezing Assets under S/Res/1373 (c. III.2):***

307. Germany implements the financing of terrorism aspects of UNSCR 1373 through EC Regulation 2580/2001 (for individuals and entities linked to non-EU States) and Section 6a of the Banking Act (for individuals and entities linked to EU States).

308. With respect to individuals or entities listed through EC Regulation 2580/2001, financial institutions and others are required to directly comply with the provisions of the Regulation by respecting the freezing of the assets without delay of the designated persons and entities without prior notice. The provisions of the Council Regulation are directly applicable law in Germany. Funds and assets are frozen directly and immediately by the Council Regulation and its amendments on the day of their entry into force.

309. The assets subject to freezing are defined in very broad terms by EC Regulation 2580/2001 (for they include funds, other financial assets, and economic resources); these assets are those belonging to, or owned or held by the designated persons or entities — however acquired. The language covers funds or other assets that are either directly or indirectly owned or controlled<sup>43</sup>.

310. It should be noted that S/RES/1373 is not fully implemented by Council Regulation (EC) No. 2580/2001, as the regulation does not apply to EU-internals. Germany overcomes this limitation by Section 6a of the Banking Act (which entered into force in November 2003). It provides that, where “known facts indicate that funds entrusted to” a financial institution or that “a financial transaction if carried out would serve” the purpose of financing a terrorist organization, the BaFin may, amongst other measures, freeze the “funds” and prohibit the institution from carrying out any further financial transactions. This provision has recently been amended by the “Act on the Prosecution of the Preparation of Serious Violent Acts Endangering the State” (Federal Law Gazette, Part 1, page 2437 et seq.) which introduced the words “the preparation of a serious act of violence endangering the State in accordance with section 89a (1), (2) number 4 of the CC or financing of a terrorist association in accordance with 129a, also in conjunction with Section 129b, of the CC.” Accordingly, the conducts of collecting, receiving, or providing of not inconsiderable assets for the perpetration of such acts is now covered.

311. According to the authorities, Section 6a of the Banking Act also established a “catch-all clause” in national legislation to combat the financing of terrorism which enables Germany to close any other regulatory gaps which may possibly be identified.

312. However, Section 6a of the Banking Act only covers credit institutions, financial services institutions and investment companies. This means that all other persons, including insurance companies, investment companies and DNFBPs, for example, are not subject to directly applicable requirements for the freezing of assets for EU-internals under S/RES/1373.

313. While the definition of “funds or other assets” contained in the EC Regulations is consistent with the definition in SR.III, questions remain as to how the freezing of assets other than funds can be implemented by financial institutions. In the case of EU-internals, where the Banking Act applies, it seems clear that freezing of assets other than funds is not being contemplated, as the Banking Act only refers to “funds.”

#### ***Freezing Actions Taken by Other Countries (c. III.3):***

314. For the lists of persons and entities designated for freezing purposes through the EU regulations, Germany has a full capacity to freeze funds in accordance with S/RES/1267 and S/RES/1373 directly through the EU regulation mechanisms. Designations from other jurisdictions are handled at EU level within the ordinary EU procedure and if accepted are implemented through amendments of Council

---

<sup>43</sup> The EU Council document entitled “Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy”, a legally non-binding document, gives an interpretation of these provisions which cover all of the cases required by international instruments.



Regulation 2580/2001. On a national level preliminary measures may be taken without delay according to the FTPA. For EU internal persons and entities not on covered by Regulation 2580/2001 the EU regime for freezing is unavailable. In such circumstances, freezing measures can be taken without delay on the basis of Section 6a of the Banking Act, (but in the case of EU-internals, only for funds, not other assets). Additionally, Germany has a court based mechanism for seizure and confiscation of terrorist funds. It is unclear however whether under this court-based mechanism Germany would be able to freeze at the request of other jurisdictions “without delay”, particularly taking into account that such mechanism would require the prosecutor to collect some degree of evidence to substantiate the suspicion for a court order to be issued.

***Extension of c. III.1-III.3 to funds or assets controlled by designated persons (c. III.4):***

315. Assets to be frozen include those owned wholly or jointly as well as those controlled.

316. As previously mentioned, the assets subject to freezing are defined in very broad terms by the EU Regulations (for they include funds, other financial assets and economic resources); these assets are those belonging to, or owned or held by the designated persons/entities – however acquired. The language covers funds or other assets that are either directly or indirectly owned or controlled. This is reiterated in the EU Best Practices Paper relating to Restrictive Measures, which provides that “the freeze covers all funds and economic resources belonging to or owned by designated persons and entities, and also those held or controlled” (para. 28 EU Best Practices Paper).

317. While the EC Regulations are not explicit on the point of joint ownership, (rather implicitly recognizing that joint ownership is a form of ownership), the EU Best Practice of April 24, 2008 relating to Restrictive Measures, which German authorities are prepared to follow, provides that “funds and economic resources jointly owned by a designated person or entity and a non-designated one are in practice covered in their entirety. The non-designated person or entity may subsequently request an authorization to use such funds and economic resources, which may include severing the joint ownership so that person’s share can be unfrozen.”

318. As mentioned previously however, in the case of EU internals, where the Banking Act applies, the freezing of assets other than funds is not being contemplated, as the Banking Act only refers to “funds”. As a result, German law is not fully in line with the standard on this point.

***Communication to the Financial Sector (c. III.5):***

319. Financial institutions and others are required to comply directly with EC Regulations 881/2002 and 2580/2001, both of which are published in the Official Journal of the European Union<sup>44</sup>.

320. Orders issued by the Ministry of Economics in the context of entities or individuals other than those listed and based on the FTPA are published in the Federal Gazette (*Bundesanzeiger*).

321. In addition, the Central Bank, usually on the same day as the changes are published in the Official Journal of the European Union or the Federal Gazette, issues circulars to all financial institutions via email indicating the relevant amendments to the restrictive measures. The circulars are available online<sup>45</sup>.

<sup>44</sup> [www.europa.eu/eur-lex](http://www.europa.eu/eur-lex)

<sup>45</sup> [www.bundesbank.de/finanzsanktionen.php](http://www.bundesbank.de/finanzsanktionen.php)



322. The authorities further stated that most financial institutions in Germany operate a computer-based financial sanctions compliance program which automatically updates the relevant lists of targeted entities and persons whose assets are frozen in a timely manner.

323. Moreover, as a service to financial institutions and others applying sanctions, the European Commission enters the details of those listed in an electronic consolidated list of persons and entities subject to financial sanctions. The consolidated list includes all individuals, groups and entities subject to asset freezing in accordance with legislation based on the EC Treaty, so its contents goes beyond the lists made pursuant to Council Regulations (EC) No 2580/2001 and 881/2002, covering also persons and entities subject to other targeted sanctions decided on in the framework of the EU Council Common Positions. (It does not include the targets of asset freezing decided by an EU Member State.) The electronic consolidated list can be downloaded from the Commission website<sup>46</sup>.

324. There is no direct legal requirement for checking customer databases against those lists. However, financial institutions and DNFPBs are bound by EC regulations and complementary German legislation. Therefore, checking and, in case of a hit, subsequently blocking funds or assets is seen as the only way of ensuring compliance with the prohibition of making funds or assets available. A check is also a prerequisite for answering a request from the *Deutsche Bundesbank* to report on any funds frozen or to give a nil report on the occasion of additions to the lists.

**Guidance to Financial Institutions (c. III.6):**

325. The competent German authorities offer online information on financial sanctions and the possibility to apply for authorizations concerning funds and assets.<sup>47</sup> An up to date information leaflet containing guidance can also be downloaded from the website of the Federal Office of Economics and Export Control. This document also refers German institutions to the EU Best Practices paper.

326. The Council of the EU provides guidance on the interpretation and application of the directly applicable EU Regulations by means of the EU Best Practices paper. The Best Practices Paper is an important piece of guidance as it ensures a uniform interpretation of the EU Regulation in all member states. The authorities have argued that Germany relies in large part on the EU Best Practices Paper to guide financial institutions and others, as the EU regulations have direct applicability to all entities and persons in Germany. This document was updated in 2008 and is publicly available on the Council website.<sup>48</sup> The German authorities inform the private sector about the availability of the EU Best Practices Paper and reference it when answering individual queries. The *Deutsche Bundesbank* informs financial institutions of changes to the EU Regulations via circular. These circulars contain instructions for reporting targeted funds.

327. The authorities stated that, due to the comparatively small number of frozen funds in Germany, no general guidance has been issued beyond the information available at the EU level. Instead, the authorities focus on case-by case counseling. Credit institutions and other parties may discuss and inquire about any issue that might arise and is not already clearly regulated by the binding legal acts from the competent authorities or the general guidance from the EU. The Central Bank and the Federal Office of Economics and Export Control maintain a telephone hotline for such questions. The Federal Ministry of

---

<sup>46</sup> [http://ec.europa.eu/external\\_relations/cfsp/sanctions/list/consol-list.htm](http://ec.europa.eu/external_relations/cfsp/sanctions/list/consol-list.htm).

<sup>47</sup> At [http://www.bundesbank.de/finanzsanktionen/finanzsanktionen\\_terrorismus.php](http://www.bundesbank.de/finanzsanktionen/finanzsanktionen_terrorismus.php) (issued by the Central Bank) and at <http://www.ausfuhrkontrolle.info/ausfuhrkontrolle/de/embargos/terrorismus/index.html> (issued by the Federal Office of Economics and Export Control )

<sup>48</sup> <http://register.consilium.europa.eu/pdf/en/08/st08/st08666-re01.en08.pdf>

Economics and Technology also regularly answers individual queries concerning the implementation of the counter terrorism measures. This approach has been chosen by the German authorities with a view to provide guidance tailored to each singular case. The Federal Ministry of Economics and Technology also gives lectures on financial sanctions at symposia and expert conferences (e.g. *Exportkontrolltag*).

328. Additional guidance to DNFBPs is addressed through circulars sent out by the Federal Ministry of Economics and Technology to industrial associations and umbrella organizations to pass the message on to their members.

329. No general guidance has been provided with respect to measures to be taken pursuant to the FTPA or the Banking Act. However, freezing orders on the basis of the FTPA themselves contain comprehensive guidance: they provide detailed motivations and explanations.

***De-Listing Requests and Unfreezing Funds of De-Listed Persons (c. III.7):***

330. Relevant European regulations do not provide for a national autonomous decision regarding delisting and unfreezing as a whole. As such, any freezing (whether pursuant to EC Regulation 881/2002 or 2580/2001) remains in effect until otherwise decided by the EU. Common Position 2001/931/CFSP of the European Union implements S/RES/1373(2001) and provides for a regular (at least bi-annual) review of the sanctions list which it has established. Moreover, listed individuals and entities are informed about the listing, its reasons and legal consequences. They are granted due process rights, including the possibility to present material which they consider sufficient for a de-listing. If the EU maintains the person or entity on its list, the latter can lodge an appeal before the European Court of First Instance in order to contest the listing decision. Requests of the German Federal Government for de-listing have to be directed through the Ministry of Foreign Affairs and its representative in the relevant UN or EU body to the UN Sanctions Committee or the European Commission. Germany has requested de-listings on its own based on conclusions from its national threat assessment. However, any person may apply for delisting as well.

331. Requests for de-listing from the UN list are directed through the German Ministry of Foreign Affairs and its representative in the relevant UN or EU body to the UN Sanctions Committee or the European Commission.

332. Delisting from the EC regulations may only be pursued before the EU courts. In the case of refusal of a request of delisting, the applicant can decide to have the matter presented to a national German court or to the European Court of First Instance and in second instance to the European Court of Justice. If the challenge is to the legality of a designation under the EC Regulations, the European Court of Justice of First Instance can hear the complaint if made within two months after the designation.

333. Designations pursuant to the FTPA or the Banking Act may be challenged under the German General Administrative Procedures Act before German courts. Challenges under the FTPA are filed directly with the competent court. Challenges under the Banking Act are first filed with the BaFin, and then the court if the BaFin does not agree to the challenge. However, no claims have been raised against provisional orders pursuant to the FTPA or the Banking Act.

***Unfreezing Procedures of Funds of Persons Inadvertently Affected by Freezing Mechanism (c. III.8):***

334. Due to the legal framework of freezing by law through directly applicable EC Council Regulations, no funds of persons that are not a designated person but bear, e.g. a name identical to, very similar to or just resembling to a name of a designated person are frozen in a legal sense. However, financial institutions may have blocked funds of such a person up until its identity is verified. In those cases, the person concerned as well as the bank may address the Central Bank or Ministry of Economics

with a request to review the case. German authorities ask financial institutions to firstly use all information available to them to verify whether one of their customers is a designated person or not. In case doubts remain despite those efforts financial institutions may address the competent authority (*Bundesbank* for funds and Federal Office for Economics and Export Control for economic resources). The relevant competent authority may consult with other EU members, the EU Council, or the UN Sanctions Committee and, if it is determined that the claim is justified, inform the bank and ask to unblock the funds. The authorities confirmed that no requests for reviewing such type of cases have been received in the past four years. Similar procedures exist for Funds frozen under the Banking Act or the FTPA.

335. The applicant can decide to sue the bank for blocking the funds before a national German court. However, the authorities confirmed that this has never occurred. If the challenge is to the legality of a designation under the regulations, the process is the same as outlined above.

***Access to frozen funds for expenses and other purposes (c. III.9):***

336. UNSCR 1267, as amended by UNSCR 1452, is implemented in the EU through a new Article 2a in EC Regulation 881/2002 — directly applicable in Germany. This provision authorizes access to funds that are frozen for basic expenses, certain fees, or for extraordinary expenses. The Central Bank and the Federal Office for Economics and Export Control are the designated competent authority to receive requests from affected persons for exemptions. Any request received is also notified to the Al-Qaida or Taliban Sanctions Committee which, within, 48 hours may object to the exemption. The competent authority must also promptly notify the person that made the request, and any other person, body or entity known to be directly concerned, in writing, whether the request has been granted or not. Before the request is granted, the competent authority has to inform other member states as well.

337. A procedure is also envisioned in Article 5 and 6 of EC Regulation 2580/2001 which relates to designations emanating from UNSCR 1373. Under Article 5 the competent authority may grant a specific authorization to unfreeze funds for essential human needs under such conditions as it deems appropriate. Article 6 establishes a broader power for competent authorities of EU member states to grant specific authorizations – with the view to protect the interests of the community and the interest of its citizens and residents – after consultations with the other member states, the Council and the Commission of the EU.

338. The authorities confirmed that no cases have been raised in connection to measures adopted pursuant to the FTPA or the Banking Act.

***Review of Freezing Decisions (c. III.10):***

339. As mentioned above, the freezing mechanisms in the relevant EC regulations can be challenged at the European Court of Justice by any natural or legal person that is directly and individually affected under the general principle established by Art. 230 of the Treaty establishing the European Community.

340. A number of appeals against freezing orders based on Council Regulations (EC) No. 2580/2001 and 881/2002 are pending in the European Court of Justice. The appeals focus on claims that the human rights of the designated individuals, groups, and entities were not respected. As regards Council Regulation (EC) No. 2580/2001, the Court of First Instance held in three judgments in 2006 and 2007 (T-228/02, People's Mujahedin of Iran (OMPI), T-47/03, Sison, T-327/03, Stichting Al Aqsa) that the Council had to provide a statement of reasons to the designated individuals, groups and entities concerned, so as to allow them to make their views known on it and to allow the court to conduct a review. These judgments are final. The Court of First Instance upheld this line of argument on April 3, 2008 in the cases T-229/02 and T-253/04, Kurdistan Workers' Party (PKK) and Kongra-Gel, which concern Council decisions made in 2002 and 2004.

341. On September 3, 2008, the European Court of Justice issued a judgment in the Kadi and Al Barakaat International Foundation cases (C-402/05 P and C-415/05 P) that annulled the 2002 EU Council regulation that implements UNSCR 1267 and successor resolutions insofar as the regulation concerned the appellants. However, the Court in essence left the EU regulation in place for up to three months to permit the European Commission to remedy the violations found by the Court. The Court found violations of fundamental human rights, specifically, the right of defense and the right to an effective legal remedy. The EU is working on an amendment to Regulation 881/2002 in order to comply with the judgment of the European Court of Justice.

342. The authorities confirmed that no cases were raised in German courts against the provisional freezing mechanism established pursuant to the FTPA or the freezing mechanism established pursuant to the Banking Act. The process described above for unfreezing funds of persons inadvertently affected by the freezing mechanisms would also apply in these cases.

***Freezing, Seizing and Confiscation in Other Circumstances (applying c. 3.1-3.4 and 3.6 in R.3, c. III.11):***

343. As noted in the analysis of criterion 3.4, professional secrecy is interpreted broadly by the liberal professions and there are strict conditions for obtaining or compelling information subject to it, which hinder the possibility for law enforcement authorities to locate and trace terrorist funds or other assets.

344. This deficiency may impact on the freezing, seizing and confiscation of terrorist-related funds or other assets in contexts other than those described under III.1-III.10.

***Protection of Rights of Third Parties (c. III.12):***

345. The rights of bona fide third parties affected by a freezing under the EU lists, Ministry of Economics freezing orders, or a seizure otherwise ordered in the German system are protected by the relevant EC Regulation as well as by the general principles of German law.

346. If the freeze is imposed through Regulation 881/2002 or 2580/2001, the bona fide third party may institute proceedings before the European Court of First Instance. EC regulation 881/2002 at Article 6 also protects the good faith actions of freezing entities except when a freeze is due to negligence. There is access to the courts in Germany to challenge aspects of a freeze that adversely affects a person or entity.

347. If the freeze has been undertaken pursuant to a decision based on the FTPA or the Banking Act, the bona fide third party can also challenge it based on the general principles of German administrative law.

348. Finally, Section 73 and 74 of the CC provide protection to bona fide third parties as the rights of third parties are not affected by a confiscation measure.

***Enforcing the Obligations under SR III (c. III.13):***

349. Both Article 10 of the Council Regulation (EC) No. 881/2002 and Article 12 of the Council Regulation (EC) No. 2580/2001 oblige member states to lay down rules on sanctions applicable to infringements of the provisions of the respective Council Regulation and ensure that they are implemented. Those sanctions must be effective, proportionate and dissuasive.

350. The penalty for violation, circumvention, or attempted violation or circumvention, of Council Regulations 2580/2001 and 881/2002 is a term of imprisonment of up to five years (see Section 34(4) of

the FTPA). Negligent violations are sanctioned with imprisonment of up to three years or fines (see Section 34(7) of that Act).

351. The *Deutsche Bundesbank* requests financial institutions by circular letter to report any frozen funds pursuant to the relevant Council Regulations (and national freezing-orders) upon entry into force of these legal acts and amendments thereto as well as thereafter from time to time on all amounts frozen. “Nil” reporting is also required. Financial institutions have to report immediately any change to the frozen amounts (due to *e.g.* the addition of interest) to the Central Bank.

352. The Council Regulations also establish certain communication and notification requirements to the competent authorities of the Member States, concerning information that can guarantee compliance as far as frozen accounts and amounts are concerned. Failure to comply with the reporting obligations is an administrative offense.

353. Financial institutions’ compliance with legislation on financial restrictions is part of the Central Bank’s supervisory program for the implementation of the FTPA. The Central Bank also has the right to demand any information required to monitor the compliance with legislative instruments of the Council or Commission of the European Communities in the field of foreign trade and payments legislation and may conduct random inspections (FTPA, Section 44). In order to carry out the inspections its staff members may enter the business premises of the persons obliged to furnish information. The Central Bank during its regular on-site inspections, examines the procedures of an institution for vetting customers against sanctions lists. This typically involves gathering information on the frequency and coverage of such checks—for example, how often is the entire client base or perhaps a proportion of it screened, how often are sanctions lists held by firms updated. Compliance with financial sanction regulations is not covered by annual audit reports of financial institutions.

354. The audit service of the Federal Customs Administration also examines, under the same Section 44, at regular intervals or based on suspicious facts, the compliance of companies with the prohibition of making funds and economic resources available to persons and entities designated by Council Regulations 2580/2001 or 881/2002.

355. In addition, the Federal Customs Administration supervises the compliance with Council Regulations 2580/2001 or 881/2002 in the context of controls on the transnational movement of goods. During import and export clearance, the Customs Administration conducts random checks, partly based on IT-supported risk analysis systems, in order to verify that the imported or exported goods are not intended for or are in the possession or property of persons, entities or organizations designated by Council Regulations 2580/2001 or 881/2002.

356. In the context of monitoring transnational cash transactions the Federal Customs Administration may temporarily seize or take into customs custody cash or equal means of payment according to Section 12a of the CCA if there are grounds to believe that the cash or equal means of payment are transferred for the purpose of financing a terrorist organization. This is in principle to be suspected if the cash or equal means of payment are in the possession or property of designated persons, entities or organizations.

357. Apart from these cases, there are no other appropriate measures to monitor effectively the compliance with the obligations of SR.III by other persons (*i.e.* lawyers, notaries, etc.). While general provisions exist for monitoring compliance with general professional obligations, including compliance with applicable laws, there are no specific measures designed to monitor compliance with SR.III obligations.

**Statistics (R.32):****Cumulative Funds frozen pursuant to Council Regulation (EC) No. 881/2002**

<b>As of 12.30.2005</b>			
Frozen funds total:		EUR 9 575.74	USD 13 326.56
Funds of 11 persons			

<b>As of 12.30.2006</b>			
Frozen funds total:		EUR 11 012.22	USD 15 325.71
Funds of 15 persons			

<b>As of 12.31.2007</b>			
Frozen funds total:		EUR 11 681.92	USD 16 257.73
Funds of 17 persons			

<b>Stand 12.31.2008</b>			
Frozen funds total:		EUR 8 953.07	USD 12 459.99
Funds of 17 persons			

**Cumulative Funds frozen pursuant to Council Regulation (EC) No. 2580/2001**

<b>As of 12.30.2005</b>			
Frozen funds total:		EUR 203.87	USD 283.73
Funds of 1 person			

<b>As of 12.30.2006</b>			
Frozen funds total:		EUR 203.89	USD 283.75
Funds of 1 person			

<b>As of 12.31.2007</b>			
Frozen funds total:		EUR 203.91	USD 283.78
Funds of 1 person			

<b>Stand 12.31.2008</b>			
Frozen funds total:		EUR 203.93	USD 283.81
Funds of 1 person			

**Additional Element (SR III) – Implementation of Measures in Best Practices Paper for SR III (c. III.14):**

358. Germany has implemented all of the measures set out in the Best Practices Paper for SR III.



359. Effective regimes and competent authorities and courts are established on EU and national level. Communication and co-operation with foreign governments and international institutions is realized on EU-level. Communication with the private sector is realized by the EU (e.g. database with designated persons and entities, EU Best Practices) and by the national authorities (e.g. websites, telephone hotlines, case-by-case counseling, information leaflets, circulars,

***Additional Element (SR III) – Implementation of Procedures to Access Frozen Funds (c. III.15):***

360. Articles 5 and 6 of Council Regulation (EC) No. 2580/2001 provide for exemptions comparable to those provided in Council Regulation (EC) No. 881/2002 as amended. They provide for the possibility to authorize the access to funds or financial assets of economic resources, if they have been determined to be necessary for the purposes set forth in Section 1(a) of the S/RES 1452 (2002). The procedure to be followed is comparable to the one for exemptions under Council Regulation (EC) No. 881/2002. However, no notification of the Sanctions Committee is foreseen. Instead, prior notification of other member states of the EU is mandatory in some cases.

**2.4.2. Recommendations and Comments**

361. In order to comply fully with Special Recommendation III, Germany should:

- Enact national legislation to implement fully Council Common Positions, No. 2001/930/CFSP and No. 2001/931/CFSP on the fight against terrorism, which are also applicable to EU-residents.
- Enact legislation to make S/RES/1373 applicable to any person (including persons other than credit institutions, financial services institutions and investment companies) for the freezing of assets concerning EU-internals.
- Set up procedures within Germany that will ensure in all cases the freezing without delay of assets other than funds (such as immovable goods, companies and businesses and vehicles); for the case of EU-internals where the Banking Act applies.
- Set up appropriate measures to monitor effectively compliance with the obligations under SRIII by persons and entities other than financial institutions and “companies”.

**2.4.3. Compliance with Special Recommendation III**

	Rating	Summary of factors underlying rating
SR III	PC	<ul style="list-style-type: none"> <li>• Except for credit institutions, financial services institutions and investment companies, no other person is subject to directly applicable requirements for the freezing of assets for EU-internals under S/RES/1373.</li> <li>• Lack of effective procedures to freeze assets other than funds for EU-internals where the Banking Act applies.</li> <li>• Professional secrecy is interpreted broadly by the liberal professions, and there are strict conditions for obtaining or compelling information subject to it, which hinder the possibility for law enforcement authorities to locate and trace terrorist funds or other assets.</li> <li>• No appropriate measures to monitor effectively compliance with obligations under SRIII by persons and entities other than financial institutions and “companies”.</li> </ul>



## Authorities

### 2.5. The Financial Intelligence Unit and its Functions (R.26)

#### 2.5.1 Description and Analysis

##### *Legal Framework:*

362. Under the German Constitution, responsibility for policing and law enforcement falls within the jurisdiction of the individual *Länder*. Section 1(3) of the Federal Criminal Police Office Act reflects that fact, stating “the prosecution and prevention of criminal offenses and the duties associated with the prevention of other threats shall remain the responsibility of the federal *Länder*, unless provided otherwise by law.”<sup>49</sup>

363. The AML Act established the FIU in the BKA on August 25, 2002. The legislation reflects a policy decision to establish the German FIU as a law enforcement model. Section 10 of the Act also sets out the mandate of the FIU as supporting the federal and *Länder* police forces in the prevention and prosecution of ML and TF, and in particular, collecting and analyzing STRs transmitted pursuant to Sections 11 and 14 of the Act; promptly informing federal and state level law enforcement authorities of information concerning them; maintaining statistics on STRs received and analyzed, follow up to those reports, cases investigated, numbers of prosecutions and convictions for ML or TF offenses and property and assets frozen, seized or confiscated; publishing an annual report; and, regularly informing reporting entities of typologies and methods of ML and TF.

364. The AML Act requires reporting entities to submit STRs to the competent authorities in their jurisdiction, namely the local Police Criminal Office (the *Landeskriminalamt*), and at the same time provide a copy of the STR to the FIU (Sections 11(1) and 14(1) and (2)). In addition, the BaFin guidance to reporting entities (paragraph 31 of the BaFin guidance of 30 March 1998) requires reporting entities also to send a copy of the STR to the BaFin for supervisory purposes; however, this guidance was abrogated by the BaFin following the enactment of the present AML Law. See Section 3 for a more detailed discussion of the status of the BaFin’s guidance.

##### *Establishment of FIU as National Centre (c. 26.1):*

365. The AML Law establishes the FIU as an element within the National Police with the mandate as noted above. Section 10 (1) of the AML Act establishes the FIU “as a central agency within the meaning of Section 2(1) of the Federal Criminal Police Act” and states that it “shall support the Federal and [*Länder*] police forces in the prevention and prosecution of money laundering and terrorism financing.” It mandates the FIU, *inter alia*, to collect and analyze STRs and to arrange cross checking of data stored by other agencies and to inform federal and *Länder* law enforcement authorities of information concerning them and on the facts of the crimes ascertained. It also mandates the FIU to cooperate and exchange information with other FIUs.

366. Bearing in mind that policing and law enforcement fall under the constitutional responsibility of the *Länder*, and considering that Sections 11 and 14 require reporting entities to submit STRs to the *Länder* police bodies with a copy to the FIU, the question arises whether the German FIU actually functions as the “national centre” or is merely a support body providing some support and information to

<sup>49</sup> This section focuses on the national FIU as required by the standard. It, therefore, does not assess any aspects of the FIU function as expected under R.26 that may be carried out by the *Länder* police.

the state level authorities who themselves conduct the analysis aimed at substantiating the suspicion of ML and terrorism financing to determine whether a full investigation should be undertaken.

367. As can be seen in the description of the processing of STRs (below), the analysis conducted by the FIU is generally not aimed at confirming and elaborating suspicions of ML or terrorism financing and determining whether a report should be disseminated to law enforcement bodies for investigation and prosecution. This type of analysis is mainly conducted by the State Criminal Police Office(s).

368. **Receipt and Processing of STRs<sup>50</sup>:** As specified in the AML Act, the individual *Länder* LEAs are the primary recipients of STRs within their jurisdiction, and the FIU receives a copy of the STR at the same time. In 14 *Länder*, the STRs are received by the *Land* Criminal Police Office, and specifically the “Joint Finance Investigation Groups — Police/Customs” within the *Land* Criminal Police Office. In two *Länder* (Hesse and Bavaria), the STRs are received by designated public prosecutor offices. As noted in the analysis of R.13, reporting entities, when reporting suspicions that involve transactions in several *Länder*, are required to split their STRs to file each part with the relevant *Land*.

369. According to the authorities, the *Land* Police unit that receives the STR is required, under Section 11(2) of the BKA law, to enter all data from the STR (including attachments) into an STR database (that is accessible to *the* joint Police and Customs financial investigation groups in 16 *Länder*, Police stations that have responsibilities in relation to combating organized crime or terrorism, and the FIU)<sup>51</sup>. When a new STR is entered into the database, the database automatically checks to see linkages to other STRs already in the database (*e.g.* common name) and all other police data bases to which the “entering LKA” has access. The *Land* police entity that receives the STR immediately commences an “investigation,” the first phase of which is the “clearing process.” This “clearing process” includes cross checking the STR information against a number of police databases and external information sources to assess whether the STR in question relates to an offense under Section 261 of the CC. It can also include more wide-ranging checks, information collection, analysis and investigative measures. If a potential link to an offense is established, and with the concurrence of the state public prosecutor, the *Land* Police “clearing office” forwards the case to the relevant investigative unit in the *Land* Police or elsewhere for further investigation. Where the STR database check reveals links to ongoing investigation(s) in other *Länder*, there is an obligation on the *Land* Police “clearing office” where the STR was originally entered to coordinate its investigation with investigators in the other *Land or Länder*.

370. At the same time, in the **first phase of the processing of STRs**, the FIU, for its part, receives a copy of the STR, reviews it for completeness, and enters it into the FIU’s restricted database which also contains FIU correspondence with foreign FIUs. The FIU does not in all cases receive all of the supplementary attachments that reporting entities may attach to the STR they send to the primary (*Land*

---

<sup>50</sup> See the discussion on R.13 for details about the nature of the reporting obligation, and the reporting practice.

<sup>51</sup> This database, sometimes referred to as the “common database,” is a cooperative initiative among the *Länder* in that each *Land* enters all of the STRs it receives in this database and remains the owner of that data, but they are accessible to the other contributors to the database, to law enforcement agencies with responsibilities for the investigation of organized crime, as well as to the Federal Police. As per s.11 (2) of the Federal Police Law, this database is managed by the Federal Police and is physically housed in the IT facility of the Federal Police, whose IT staff performs the database maintenance and administration functions on behalf of the owners of the data (the *Länder* Police bodies who enter their data into this database).

Police) recipient<sup>52</sup>. Nonetheless, the FIU is the “national center” for receiving STRs<sup>53</sup>, and in a narrow sense, meets this aspect of the requirements for an FIU in R.26.

371. The FIU automatically checks the STRs it receives against all other reports and foreign FIU correspondence received to that date, and can also check other relevant BKA intelligence databases to which it has access but which are not necessarily accessible to the *Land* Police. When appropriate, the FIU may also seek and obtain information from foreign FIUs. If any of these checks yield relevant information, the FIU forwards the information to the *Land* Police unit that is conducting the “clearing process” or the subsequent investigation (while observing any restrictions on dissemination that may attach to any of the information received from foreign FIUs). The authorities stated that the FIU has direct or indirect access to a number of other governmental and commercial databases, though it is unclear to what extent such sources are regularly or routinely accessed in practice for case analytical purposes.

372. Any STRs that identify suspicion of TF, as well as others that the FIU may identify as possibly being relevant to TF, are immediately forwarded by the FIU to the Terrorist Financing Unit of the BKA. FIU staff also indicated that three members of the Terrorist Financing Unit of the Federal Criminal Police have direct access to the FIU database.

373. The **second phase of the processing of STRs**, described by the FIU as “monitoring.” focuses on identifying and categorizing STRs in the following groupings:

- Prominent cases (involving persons of business, political or other prominence);
- Indications of TF (as already noted, these reports are immediately forwarded to the Terrorism Financing unit of the BKA);
- Trends;
- Typologies; and
- Reports of no relevance.

374. In effect, the processing of STRs is divided between the *Land* Criminal Police Office recipients of the STRs, and the FIU. The former undertakes analysis and investigation to determine whether there are sufficient grounds to undertake a full investigation of ML or terrorism financing. The FIU for its part conducts checks against its own database of all previous STRs as well as searching other relevant BKA databases. It also initiates the exchange of information with foreign FIUs. Relevant information yielded by these processes is forwarded to the *Land* Police entity that received the STR.

375. The authorities indicated that Germany had adopted its dual *Länder* and FIU approach for receiving and analyzing STRs to respect the constitutional role of *Länder* police to investigate crime and to determine whether there are grounds to suspect ML or TF to begin an investigation. In addition, they indicated that this arrangement facilitates the prompt application of any necessary measures, inter alia freezing suspicious assets or obtaining an injunction under the CPC to prevent execution of a transaction. A further benefit of the dual database approach that they cited relates to the fact that, under the Data

<sup>52</sup> The authorities state that once an electronic suspicious transaction reporting process is implemented, the FIU will receive STRs and all attachments.

<sup>53</sup> Pursuant to a BaFin Guideline of 1998, financial services institutions are required to provide a copy of their STRs to BaFin for compliance monitoring purposes.

Protection Act, there are different file opening and data retention rules applicable to case files of *Länder* Police investigative units and the intelligence files of the FIU. The FIU data can be retained for up to four years, even if the investigative file has been closed and deleted from the *Länder* (“common”) police database (a requirement under S.32 (2) 9(1) of the BKA Law if investigations establish that there is no residual suspicion of any crime, which is the case in about five percent of investigations)..

376. The practical effect of the arrangements described above is that the FIU does not conduct the full analysis of STRs and related information to determine whether there are sufficient indications of ML, and, dissemination of the STR(s) and analytic reporting to a law enforcement body for investigation. Analysis of STRs to substantiate suspicion of ML is performed primarily by the Police unit in the *Land* that first receives the STR. The FIU can and does provide supporting information from its sources to the unit carrying out that analysis. The FIU does in some few special cases conduct such analysis. Moreover, based on the BKA jurisdiction in matters related to terrorism, the FIU reviews incoming STRs for those that specifically address suspicions of TF, as well as ML STRs that appear to have a possible connection to TF, and forwards those to the Terrorist Financing Unit of the BKA.

***Guidelines to Financial Institutions on Reporting STR (c. 26.2):***

377. The FIU itself has no authority to issue direction as to form and manner of reporting. The BaFin, as part of broader guidance to financial entities under its supervision, issued guidance in 1998 (Guidelines concerning measures to be taken by financial services institution to combat and prevent ML) as to form and manner of reporting suspicious transactions made as per Section 11 of the AML Law.

378. After wide consultation, the FIU has developed a “standard STR reporting form” which was published in the Annual Report of 2004, complete with instructions for completing it. Use of this form is not mandatory. Only about half of reporting entities use this format. There are no plans to make the use of the standard format obligatory (an issue that may limit the effectiveness of an electronic reporting initiative that is planned for 2010). The absence of an obligatory standard reporting format makes data entry more time consuming, and comparative analysis more difficult. It may also increase the risk of receiving incomplete or inaccurate information.

***Access to Information on Timely Basis by FIU (c. 26.3):***

379. The FIU, being part of the BKA, has direct access to law enforcement information as well as timely direct, usually on-line, access to a number of governmental and non-governmental information sources, including persons registries, drivers’ license and motor vehicle registries. Access to an automated account access system operated by the BaFin is indirect (see section 7.2 below of this report for more detailed information). The FIU may also access commercially or publicly available databases, normally on-line, as well as information from Interpol, Europol, liaison officers of the BKA abroad, and foreign FIUs through FIU.net and the Egmont secure web.

380. Assessors were informed that, in practice, because the process of carrying out the screening and analysis of STRs and amplification of information related to them is already being carried out at the level of the *Land* Police, the FIU generally checks those databases and information sources that contain information from foreign sources to which the *Land* Police do not have access. If relevant information is found in those checks, it is communicated to the relevant *Land* police unit for that unit’s case work.

***Additional Information from Reporting Parties (c. 26.4):***

381. The FIU has the power, indirectly, to obtain additional information from reporting entities. The FIU states that there is no need for the FIU to exercise this power because the relevant *Land* Police unit

that has carriage of the investigation will itself seek any additional information it needs from the reporting parties by way of a request for information from the public prosecutor's office (per Section 161a of the CPC). (While the authorities stated that the FIU does have the lead investigative role in some few cases, they were unable to provide statistics on the number of cases, per year, for which the FIU takes the lead investigative role, and the number of times per year the FIU seeks additional information from reporting entities).

***Dissemination of Information (c. 26.5):***

382. Section 10 (1) 1 and 2 specify that the FIU shall: "1. Collect and analyze STRs transmitted pursuant to Sections 11 and 14, and in particular arrange for cross checking of data stored by other agencies," and, "2. inform the Federal and [*Länder*] law enforcement authorities of information concerning them and on the facts of the crimes ascertained." STRs are submitted by reporting entities directly to the relevant *Land* Police, with copies sent at the same time to the FIU. The *Land* Police conducts its own analysis and checks of other data bases and external information sources.

383. As already noted above, the FIU routinely checks incoming STRs against its database of previously received reports, and also checks BKA databases to which the *Land* Police may not have access. Information yielded by these searches is forwarded to the relevant *Land* Police unit. Similarly, any information obtained from foreign FIUs and held by the German FIU may, subject to any caveats applied by the FIUs that provided the information, be shared with the relevant *Länder* level investigative authorities.

384. The FIU does not, as such, disseminate financial information reports on suspicions of ML to domestic investigative bodies. The FIU states that there is no need for the FIU to disseminate such information to the *Länder* police agencies, because those agencies already have the same information, and conduct their own analysis and investigation.

385. With regard to STRs either specifically filed because of suspicions of terrorism financing, or because the FIU's examination indicates a TF connection of a report filed as a suspected ML report, the FIU forwards such reports and additional information it may have in relation to them to the terrorism financing section (ST45) of the State Security Division of the BKA. The FIU has granted access to the FIU database to three designated officers of the BKA State Security Division for the purposes of investigating potential cases of terrorism financing.

***Operational Independence (c. 26.6):***

386. The FIU carries out its functions as provided by its mandate (described above). It is not subject to outside direction as to its own operational functions, makes its own decisions about the processing of incoming STRs and the disclosure of appropriate information to other investigative bodies or prosecutors. The authorities stated that, since the FIU is a police unit, it can sometimes, though infrequently, be called upon to participate in an investigation. However, the authorities were unable to provide statistics as to the frequency of such cases). To the extent that the FIU becomes involved in a criminal prosecution, it is subject to the direction of a prosecutor, and subject to the principle of mandatory prosecution.

387. The FIU's database is only accessible to FIU staff (and, as already noted, to three TF investigators). The FIU is not required to provide any special reports to more senior officers of the BKA who do not have responsibility for ML or TF issues. The Head of the FIU is appointed for an indefinite period by a competitive process from within the ranks of the BKA. FIU staff is recruited by competition, from members of the BKA or staff of the Ministry of the Interior. The Head of the FIU is able to choose



new staff members, although staffing decisions ultimately fall within the scope of the Federal Criminal Police Human Resources Administration.

388. The FIU, as a unit of the BKA, does not have an independent budget. Funding and services are provided by the BKA. Budgets are set through a process of request, consultation, and negotiation.

***Protection of Information Held by FIU (c. 26.7):***

389. The FIU reports that approximately 99 percent of STRs are submitted electronically by fax. Transmission from reporting entities to the FIU takes place via commercial fax facilities. The data are captured and stored in the FIU database. STRs that are received in hard copy are digitized and also captured as electronic documents in the FIU database. No information was provided as to the secure storage of any hard copy records of the incoming faxes. Information sent from the FIU to the *Länder* Police Offices is transmitted via a separate and encrypted police communications network.

390. The FIU has established an independent database of STRs and related “information of legal relevance as well as information exchanged or received from foreign FIUs.” This database is held on a stand-alone server located in the IT department of the Federal Criminal Police. Unique passwords are assigned for access and all systems are reported to be equipped with updateable access control mechanisms and means to differentiate access depending on a user’s authority and requirements. Access to this database is controlled, and logged, and the FIU stated that the logs are regularly reviewed. The assessors were informed by the FIU that the controls on the information were reviewed positively by the Office of Data Protection in 2004.

391. The assessors reviewed the technical specifications developed for the creation of the database which show that on average one out of every ten accesses of the database (selected at random) is automatically logged and that the logged information is retained for 12 months. Assessors were of the view that it may be preferable to log all access for detection of unauthorized access or browsing by employees or other persons that may have or gain access to the data base. Authorities subsequently indicated that by the end of 2009 all queries are expected to be logged automatically.

392. With two exceptions, only FIU employees have authorized access to the database, and access is granted on a need to know basis (not all FIU staff have access to all categories of information). The database administrator in the IT department has access to the system. In addition, one outside operational entity has access to the FIU’s data base, specifically the Terrorism Financing unit (ST45) of the Division of State Security of the Federal Criminal Police. The FIU indicated to assessors that three specifically named staff members of ST45 (recently reduced to two with the departure of one of the designated investigators) are indoctrinated to the sensitivity of the information (including the foreign sourced information) and are permitted access to the database for terrorism financing investigation purposes only. The FIU also states that use of any information provided by foreign FIUs that is identified by the designated terrorism financing investigators still requires the approval of the providing FIU.

393. Assessors visited the FIU’s premises with the Head of the FIU, after normal business hours. The FIU is part of the “Commercial and Financial Crime” subdivision housed in the building (W-8). Entry to the premises is governed by BKA security office regulations and access is controlled on a 24/7 basis. Visitors are screened and have to be escorted. The FIU section is not closed off from other sections of the building and there do not appear to be special access controls to the FIU’s section(s) of the area, over and above those performed at the entrance to the building. Assessors noted that persons in possession of BKA passes could enter the building freely, and because of the lack of physical barrier around the FIU premises, presumably could also enter the FIU section at will. The individual offices in the FIU section were not locked, and their doors to the corridor were open. Assessors were informed that all computers and files had

already been completely locked. They did not notice significant amounts of papers or reports on desktops or on tables, nor were computer terminals left turned on, and there appeared to be locked cabinets in each of the offices. The street level entrance to the building is controlled by a security officer, and there are facilities for checking hand luggage. Authorities indicated that it is planned to move the FIU to more self-contained premises in which it will be easier to implement special access controls to the FIU.

394. FIU positions are staffed by competition from a pool of eligible employees (those already members of the Federal Criminal Police or staff of the Federal Ministry of the Interior). Both of those organizations conduct intensive screening, including reliability and integrity checks, of all employees entering the organization and renew that screening at regular intervals. In addition, those staff members of the FIU who may require, or have, access to particularly sensitive information are also subjected to a security clearance screening procedure before gaining access to classified material.

***Publication of Annual Reports (c. 26.8):***

395. Section 10 (1) 5 of the AML Act spells out one of the FIU's mandate elements as: "regularly inform the persons obliged to report on types and methods of money laundering." In this regard, the FIU prepares reports about emerging ML trends, and new typologies, which are transmitted to reporting entities, posted to the password protected secure area of the FIU website section that is reserved for reporting entities, or both. Many of them are also published in the Annual Report, which is accessible to reporting entities on the FIU website. Because this information is communicated in several different ways to reporting entities and others, there are no data available as to the number of such reports issued annually.

396. The FIU publishes comprehensive annual reports containing a wide range of statistical information. These are posted to the FIU's public website in German and English. In addition to the annual reports, the FIU also issues a number of special reports on new trends and typologies based on its own strategic analysis. It also publishes periodic newsletters, of relevance to law enforcement partners and financial reporting entities. Some of those reports and bulletins, sometimes in sanitized form, are also posted to the FIU's public web site. Several of the FIU's partner agencies commented positively on these Annual Reports and newsletters. Assessors also found them to be useful sources of information about the broader AML/CFT regime.

397. The FIU Newsletter is intended to inform all entities subject to the reporting requirements of the ML Act of current developments in the field of suppressing ML. Since this initiative was launched in 2005, seven FIU Newsletters have been issued.

398. Access to the password protected secure area of the FIU website is intended exclusively for ML officers of reporting entities. ML officers are required to show proof of their appointment to their association or the FIU in order to obtain access to the restricted section of the web site. The restricted site contains information such as the STR form together with instructions for use, etc.

***Membership of Egmont Group (c. 26.9):***

399. The German FIU has been an active member of Egmont since 2003.

***Egmont Principles of Exchange of Information Among FIUs (c. 26.10):***

400. Section 10 (2) of the AML Act requires the FIU to cooperate with the FIUs of other countries responsible for the prevention and prosecution of ML and TF. In practice this has been deemed to mean FIUs that are also members of Egmont. The FIU frequently exchanges information with foreign FIUs, and,



in doing so, adheres to the Egmont Principles (with the possible exception of the above noted data base access by designated TF investigators).

401. The German FIU is not required to conclude MOUs for information exchange with other FIUs, but is able to enter into such MOUs with FIUs that may require them. Section 10(4) of the AML Act indicates that the FIU may use data provided by foreign FIUs solely in line with the conditions imposed by the sending FIU, and the German FIU may impose its own restrictions and conditions on the use of information transmitted by it to the FIU of another country.

402. Information exchange with foreign jurisdictions is a prominent feature of Germany's AML/CFT regime and the FIU plays an important role in that. In 2008, for example, the FIU engaged in 773 exchanges (677 enquiries from abroad and 96 German requests to foreign FIUs). These exchanges involved the German FIU and 75 foreign FIUs.

#### BKA FIU Information Exchange with other FIUs

Year	Number of Information exchanges
2003	482
2004	606
2005	667
2006	737
2007	744
2008	773

Source: BKA Annual Reports 2004 – 2007.

\*in 2007 the total number consisted of 653 enquiries from abroad and 91 German requests to other FIUs.

\*\* 2007 Annual report notes exchanges took place with 71 foreign FIUs.

\*\*\* Top 20 exchange partners accounted for 581/744 exchanges or 78% of total.

#### *Adequacy of Resources – FIU (R. 30)*

403. The FIU has 18 staff, not including the Head of the FIU. Eleven are investigators, and seven are administrative employees. The Unit also has access to some external consultants for problems that require expert knowledge in areas in which the police are not sufficiently knowledgeable. These persons are used on a contract basis. They do not have access to operational information.

404. The FIU is a unit of the Federal Criminal Police. As such, it does not have its own separate budget. Its resources are provided by the larger organization, and consist mainly of salaries and the cost of materials, travel, and the management of the necessary information technology. Administrative support, accommodation, IT services, and security are supplied by the Federal Criminal Police.

405. Positions in the FIU, including the position of Head of the FIU, are staffed through a competitive selection process from a pool that consists of serving BKA officers and officers of the Ministry of the Interior. Positions are not normally staffed from outside that pool. Prospective police candidates must have completed a three-year university course and graduated with the rank of detective chief inspector. They must possess some basic understanding of financial crime and ML. Successful candidates undergo a program of orientation training on arrival at the FIU and are also assessed as to their general knowledge of the field and then provided with appropriate training depending on their specific needs.

406. A wide range of training programs is available to staff on a continuing basis, including such subjects as operational and strategic analysis, financial investigations, economic crime, asset confiscation, etc.

407. The resources allocated to the FIU have increased substantially in the past 4-5 years. Information processing and data entry requirements consume a substantial portion of those resources. Mandatory standardized reporting and fully automated electronic reporting would ease those resource pressures. The current analytic function of the FIU is mainly focused on strategic analysis, and thus not quite as time sensitive as operational analysis, would be. A substantial increase in the number of STRs reported, or an expansion or intensification of the FIU's role in tactical and operational analysis would require additional resources. The present allocation appears to be adequate for the current level and scope of functions performed.

**Statistics (R. 32):**

408. The FIU collects and analyses a wide range of statistical information, much of which is published in its annual report, as well as other publications. This includes:

- Numbers of STRs, by reporting entity type;
- References to possible predicate offenses;
- Results of police processing of STRs;
- Origin and destination of asset transfers;
- Origin of suspects in STRs;
- National and international cooperation; and.
- Analysis of follow-up responses by prosecutors' offices.

409. The FIU annual report contains a wealth of statistical tables that provide a wide range of useful information for the purposes of reporting the results of the AML/CFT regime. It also provides information about trends and typologies.

410. The FIU does not, however, record or hold in its database information on the values involved in the transactions that have been reported in STRs. It does flag some "special cases" where the transactions involve significant sums *e.g.* in excess of EUR 1 or EUR 2 million (USD 1.4 or USD 2.8 million).

**Analysis of Effectiveness**

411. There are several factors that limit the effectiveness of the FIU and of the functions set out in R. 26.

- With only a few exceptions, the FIU does not lead the process of analysis of STRs for the purpose of substantiation of suspicions. It makes only a modest contribution to the substantiation of suspicions of ML or TF by *Länder* Police units. The FIU enters STRs into a database and checks incoming reports against that FIU database, sometimes seeks information from foreign FIUs, and forwards relevant information to the *Länder* Police Office that is conducting the "clearance process" or investigation.
- *Länder* police and prosecutorial officials noted that the FIU's contribution to the "clearance process" is not significant (although it was acknowledged that the FIU's access to information from foreign FIUs does at times make a helpful contribution).

- The reporting process is not efficient. The FIU has endeavored to provide some guidance to reporting entities to improve efficiency by elaborating a “standard” reporting format, but there has been only modest success in getting reporting entities to adopt this format. This increases the risk of incomplete reporting, and complicates analysis, both for the FIU and the *Länder* Police units that receive the STRs. The FIU is more effective in its analysis of STRs for the purpose of identifying trends, patterns and typologies (though as noted, this analysis is hampered by the FIU not having data about transaction values), and distributes reports of this nature to reporting entities and to investigative bodies, though no data were provided as to the numbers and frequency of such reports.
- Although the FIU has authority to access a range of governmental and non-governmental information sources, the extent of the use of that authority is not clear. The FIU indicates that all incoming STRs are checked against its own and other police databases. Access to other external (governmental, commercial, or public) data sources appears to be less frequent. Data on the frequency of access to such data sources were not available.
- The absence of secure automated transmission facilities for the submission of STRs by reporting entities complicates the process of receiving and uniformly entering the data in the FIU database and the use of the data for analytical purposes.
- The available statistical information does not make it possible to show how many STRs (if any) are linked to convictions of ML or to confiscation of proceeds.

412. In summary, it was not established that the German FIU functions as an FIU in complete compliance with the standard. Rather, it appears more to be an agency to provide some support to *Länder* Police who have lead responsibility both for the substantiation of suspicions of ML or TF and any ensuing investigation. The FIU provides some information from its own databases to the investigating *Länder* Police. It is also involved in sharing and receiving information with or from foreign FIUs. It focuses its analytic work on the elaboration of patterns and trends, information that it disseminates to reporting entities and investigative bodies.

### **2.5.2 Recommendations and Comments**

413. In order to comply fully with Recommendation 26, Germany should:

- Strengthen the capacity of the FIU to act as a national centre for receiving, analyzing, and disseminating to law enforcement and other appropriate agencies financial information about suspected ML and TF, more consistent with the standard enunciated in R.26, in particular, by having the FIU carry out more robust analysis of STRs directed towards disseminating information to *Länder* Police when the FIU concludes that there are grounds to suspect ML or TF.
- Strengthen the FIU’s tactical analytic capacity through increased personnel and training.
- Equip the FIU with the authority to provide direction to reporting entities as to the manner and form of reporting suspicious transactions to the FIU and implement a standardized, more automated reporting system for STRs.

### 2.5.3. Compliance with Recommendation 26

	Rating	Summary of factors underlying rating
R. 26	LC	<ul style="list-style-type: none"> <li>• FIU is only one of many centers that receives, analyzes, and disseminates STRs and other relevant information concerning suspected ML or TF activities.</li> <li>• The FIU carries out limited case-specific analysis of STRs, and less than ten cases each year where that analysis is directed towards informing a decision about whether to disseminate information to domestic authorities for investigation on the basis that there are grounds to suspect ML or TF.</li> <li>• Overall effectiveness of the FIU function as expected under R.26 is or may be compromised by: <ul style="list-style-type: none"> <li>○ Guidance to reporting entities on form and manner of reporting is not sufficiently strong and information is received and accepted in a variety of formats and through various channels.</li> <li>○ Data in STR attachments sent to LEAs are not always available to the FIU for entry into the FIU database and thus not always available for analysis.</li> <li>○ No information in FIU database about value of transactions in STRs.</li> <li>○ No ongoing national coordination or management of tactical analysis of STR information.</li> <li>○ Inability to produce statistics on STRs analyzed or disseminated or linked to a prosecution or conviction of ML and confiscation of proceeds.</li> </ul> </li> </ul>

## 2.6. Law enforcement, prosecution and other competent authorities – the framework for the investigation and prosecution of offenses, and for confiscation and freezing (R.27, & 28)

### 2.6.1. Description and Analysis

#### Legal Framework:

414. The responsibilities, rights and duties of the law enforcement and prosecution agencies are predominantly set forth in the CPC (*Strafprozessordnung*, StPO), the CC (*Strafgesetzbuch*, StGB) and the police laws of the individual States. German prosecution authorities have the authority and responsibility to ensure that all offenses, including the ML and TF offenses, are investigated and prosecuted. Criminal investigations are carried out under the direction of the public prosecutor. Pursuant to the principle of mandatory prosecution, established under Section 152 (2) of the CPC, the “public prosecution office” is obliged to take action in relation to all criminal offenses which may be prosecuted, provided there are sufficient factual indications.

#### Designation of Authorities ML/TF Investigations (c. 27.1):

#### Money laundering:

415. Responsibility for the investigation and prosecution of ML lies mostly with the police and prosecutorial authorities of the *Länder*, each of which has its own *Land* criminal police office and its own *Land* prosecutors. Where there are international dimensions to the investigations, the BKA coordinates the efforts to seek the cooperation and support of foreign investigative bodies.

416. An investigation into an ML conduct may be initiated by an STR, a criminal complaint (other than an STR), or in the context of an investigation regarding the predicate offense.

417. STRs from obliged reporting entities are submitted to the relevant *Land* police entity and simultaneously to the FIU. Under the direction of the prosecutor of that jurisdiction, the police undertake a preliminary investigation, or “clearing process” to determine whether there are sufficient indications of ML to warrant a full investigation. Based on the results of that process, the prosecutor decides whether further investigation is to be undertaken and which investigative body will be tasked to carry out that investigation. The prosecutor directs the investigation and determines whether charges will be brought, and if so, what those charges will be.

418. All *Länder* police agencies have dedicated units that undertake the “clearing” investigations. In addition, most also have financial investigation units that undertake, among other financial crime investigations, the investigation of ML offenses. In all instances, these are Joint Financial Investigation Groups made up of police officers and customs investigation officers. Some states, among them Berlin, have developed specialized and sustained ML investigative groups.

419. At the federal level, the BKA has responsibility to support the *Länder* police bodies through the provision of specialized services, including investigative specialties, and forensic service, as well as liaison with foreign law enforcement entities where there is an international dimension to investigations.

### **Terrorist Financing**

420. The allocation of responsibilities for investigating and prosecuting terrorism are more complex, as both federal and state level police bodies and prosecutorial units have roles and there can be several agencies involved at both the federal and state levels. Both levels have ministries of the Interior and domestic intelligence agencies potentially involved in such cases. In purely domestic cases, the state level police and intelligence bodies will take the lead. If there is an international dimension, the *Länder* bodies may seek the involvement of the BKA, or, if the nature of the activity meets the test of federal responsibility of s. 4(1) and 4(2) of the Federal Police Act, the Federal Police will have lead responsibility.

421. There is a high degree of cooperation among federal and state bodies involved in investigations of terrorism and terrorism financing, and there are a number of bodies that meet with high frequency and regularity at the Joint Counter-Terrorism Centre Task Force (GTAZ) in Berlin to coordinate approaches and strategies, and in some instances to carry out joint or combined investigations. The GTAZ is the principal entity for coordinating and sharing information about terrorism and TF. The GTAZ houses approximately 220 specialists from the police (including the Customs Criminological Office (ZKA)), intelligence services, the Public Prosecutor General at the Federal Court of Justice (GBA) and the Federal Office for Migration and Refugees (BAMF) working together to conduct, *inter alia*, background analyses and intelligence support analyses in the area of Islamist terrorism. At any time, there are representatives of as many as 40 German intelligence and investigative bodies present.

422. At the federal level, a dedicated unit of the federal criminal police, ST 45, is the specialized department for the financial investigation of politically-motivated crime. It is also the competent national authority for financial sanctions as set out in Regulations EC 2580/2001 and EC 881/2002. In this capacity, it is involved in listing and delisting terrorist suspects and organizations and initiates asset freezes under the Banking Act, S.6a.

423. The Federal Office for the Protection of the Constitution (BfV, domestic intelligence agency) and the Federal Intelligence Service (BND, foreign intelligence agency) also play a key role in investigating TF. Their duties and powers are governed by the Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution (*Bundesverfassungsschutzgesetz*, BVerfSchG) and the Act on the Federal Intelligence Service (*Bundesnachrichtendienstgesetz*), as well as the Act to restrict the Privacy of

Correspondence, Posts and Telecommunications (concerning telecommunications surveillance). Both of these agencies are represented at the Joint Counter-Terrorism Centre (GTAZ).

***Ability to Postpone / Waive Arrest of Suspects or Seizure of Property (c. 27.2):***

424. While the authority to postpone or waive the arrest of suspected persons, or the seizure of the money or both, is not expressly found in a law or similar measure, Germany's law enforcement and prosecutorial authorities implement these measures in practice. Decisions to arrest or seize, or do both, are subject to tactical considerations and could be postponed to aid further investigations or to avoid interfering with the prosecution of a crime.

425. The public prosecutor's office may decide at its discretion at what point in time during a preliminary criminal investigation the issuance of a warrant of arrest is appropriate, or at what time it requests to have such an order repealed. The ability to postpone the arrest of suspects or the seizure of property can be exercised in the context of controlled deliveries or undercover operations.

426. Assessors were not able to confirm whether this power is being used in Germany effectively as the authorities did not provide statistics on the frequency with which this measure is being applied.

***Additional Element – Ability to Use Special Investigative Techniques (c. 27.3):***

427. The following special investigative techniques are permitted:

- Telephone taps (Sections 100a *et seq.* of the CPC).
- Use of undercover agents (Sections 110a *et seq.* of the CPC).
- Use of informants (regulated in the individual guidelines for conducting investigations issued by each of the *Land* Prosecution Offices).
- Use of controlled deliveries (regulated in the individual guidelines for conducting investigations issued by each of the *Land* Prosecution Offices).

***Additional Element – Use of Special Investigative Techniques for ML/TF Techniques (c. 27.4)***

428. No statistics are kept on the use of special investigative techniques for combating ML or TF other than telephone interceptions. The authorities stated that German law enforcement agencies generally use all available investigative techniques to investigate crimes (see above). Telephone interception is permissible for ML (Section 100a (2) no. 1m of the CPC) and TF (Section 100a (2) nos. 1a and 1d of the CPC). The use of undercover investigators is permissible in the area of TF pursuant to Section 110a (1), first sentence, no. 2 of the CPC, and for ML pursuant to Section 110a (1), sentence 1, nos. 3 and 4 of the CPC, for ML involving aggravating circumstances.

429. The data for telephone-interceptions is collected by the Federal Office of Justice. The number of investigations where telephone interceptions based on Section 100a of the CPC was applied and where ML has been the reason or at least one reason (Section 100a. (1), no. 2 of the CPC) to apply this measure is listed in the following table:



Year	2005	2006	2007	2008*	Total
Investigations	48	40	45	93	226

\*The data for 2008 does not refer to the number of investigations but to the number of rulings for telephone interceptions. As there can be more than one ruling in an investigation, the number has increased. The change in statistics is due to the new Section 100b (6) of the CPC that explicitly states what data has to be collected.

***Additional Element – Specialized Investigation Groups & Conducting Multi-National Cooperative Investigations (c. 27.5):***

430. Specialized investigation groups exist at both the level of the states, which have primary responsibility for investigating ML and terrorism financing, and at the federal level, including:

- Money laundering “clearing offices” (state level);
- Joint Financial Investigation Groups, (state and federal);
- Asset recovery offices (state and federal); and
- Specialized anti money laundering investigation units (several states).

431. At the international or multinational level, the BKA is the designated body to cooperate with law enforcement agencies of other countries. Cooperative action is normally undertaken on the basis of a request for mutual legal assistance. The FIU (located in the BKA) is designated and required to cooperate with the financial intelligence units of other countries.

***Additional Elements – Review of ML & TF Trends by Law Enforcement Authorities (c. 27.6):***

432. The authorities did not provide any information about formal system-wide reviews of ML and TF trends. One of the core elements of the central agency functions of the BKA and BfV is to produce a situation report covering current modus operandi and analyzing trends in TF. The production of such reports requires regular meetings to be held and a close coordination among agencies.

433. More informal review, however, takes place in a number of fora. ML investigations involve “joint financial investigation teams” at Federal and *Länder* level, comprising police and customs investigation officers. In addition to handling specific investigations, these inter-agency cooperative arrangements allow for the exchange and analysis of experiences and intelligence on methods, trends and techniques of ML.

434. Round-table discussions and project ‘managers’ meetings involving the federal and state agencies that deal with combating ML and TF are held regularly (*e.g.* meetings of the heads of the financial investigation offices, meetings of the heads of the asset recovery offices, project managers' meetings on politically motivated crime etc.). A specific element of these meetings is the discussion and sharing of information among participants about emerging trends in ML and TF, new practices and effective techniques for dealing with them and experiences as to successful approaches or challenges that need to be met.

435. In appropriate cases, intelligence relevant to TF is also exchanged between agencies at the Joint Counter-Terrorism Centre (GTAZ) in Berlin. This center was established in December 2004 as a platform where all state and federal agencies involved in combating radical Islamic terrorism work together, exchange information in real time, prepare joint analyses and coordinate operational responses.



***Ability to Compel Production of and Searches for Documents and Information (c. 28.1):***

436. Law enforcement agencies have all overt and covert criminal procedure measures available to them in order to clarify the facts and gather evidence in investigations and prosecutions of ML, TF, and other underlying predicate offenses, or in related actions, such as actions to seize, freeze, forfeit and confiscate the proceeds of crime, including:

- Powers to compel the production of objects (Section 95 CPC); this includes all of the records, data, files, documents, and information referred to under criterion 28.1;
- Requests for information by the public ‘prosecutor’s’ office to other competent authorities (*e.g.* in order to obtain account records through the BaFin etc., Section 161 of the CPC);
- Searches of persons and property of the suspect and other persons (Sections 102 and 103 of the CPC), usually on the basis of a court order;
- Seizures or freezing of evidence (Sections 94 *et seq.* of the CPC), usually on the basis of a court order;
- Asset recovery (Section 73 *et seq.* of the CC and Sections 111b *et seq.* of the CPC);
- Telephone interception (Sections 100a *et seq.* of the CPC), usually on the basis of a court order;
- Questioning witnesses or accused persons (*e.g.* Sections 58 *et seq.*, 133 *et seq.* and 161 *et seq.* of the CPC); and
- Use of undercover agents (Section 110a *et seq.* of the CPC).

437. Public prosecutors may, if there are actual indications of unconstitutional (particularly terrorist) undertakings seek information from credit institutions, financial services institutions and finance companies in relation to accounts, account holders and other beneficiaries, other parties involved in payment transactions, and cash movements and investments (particularly account balances and incoming and outgoing payments). However, this power may only be exercised in such specific cases and the information gathered may only be used in the context of such cases.

***Power to Take Witnesses’ Statement (c. 28.2)***

438. Pursuant to Sections 58 *et seq.*, and 161 *et seq.* of the CPC, the competent authorities referred to above have the powers to be able to take witnesses’ statements for use in investigations and prosecutions of ML, TF, and other underlying predicate offenses, or in related actions. These basic powers are used routinely in most cases.

***Adequacy of Resources to Law Enforcement and Other AML/CFT Investigative or Prosecutorial Agencies (c. 30.1)***

439. The primary law enforcement agencies in Germany are the public prosecutor’s offices and the police (*Land* Police and the BKA). However, other law enforcement agencies include the Customs Administration and, for tax matters, the Tax Authorities with their tax investigation units. These agencies have police investigative powers and usually work under the direction of the *Land* or Federal public prosecutors.

440. The Federal Prosecution Office based in Karlsruhe plays an important role in the prosecution of terrorism financing. It is supported by 229 employees in total, including 104 prosecutors (in 2008). The Federal Prosecution Office consists of 3 Divisions, one of which, the Division terrorism with 8 sub-divisions, is relevant to the prosecution of TF. In 2009, the volume of the budget of the Federal Prosecution Office was nearly EUR 21 million (USD 29 million).

441. As the federal center for German police, the BKA, with its approximately 5 500 employees, is responsible for coordinating the national fight against crime in close cooperation with the State Bureaus of Criminal Investigation, and for conducting investigations into certain serious crimes with a foreign connection. The BKA also represents the Federal Republic of Germany as its National Central Bureau within Interpol. The BKA receives funding out of the federal budget. The volume of the budget of the BKA was approximately EUR 362 million (USD 504 million).

442. The BKA consists of nine large Divisions, two of which are relevant to ML and TF: SO–Organized and Serious Crime; ST–State Security. The SO division (Economic and Financial Crime) consists of 5 sub-divisions. The subdivision SO 3 (Economic and Financial Crime), consist of 6 sections. In Section SO 32 (Money Laundering, Joint Financial Investigation Group, FIU), the FIU is embedded as a special subsection.

443. At the *Länder* level, there are 245 staff involved in the Joint Financial Investigation Groups that investigate ML or TF, but no information on funding was disclosed. No organization charts were provided for *Länder* level police bodies. Nor was any information provided to allow the assessors to determine whether the *Länder* police have sufficient operational independence and autonomy to ensure freedom from undue influence or interference. This lack of information is pertinent to this assessment given that the *Länder* police carry out most of the analysis of STRs to determine whether grounds to suspect ML or TF exist.

444. The FIU's work is supported by the 245 employees in total (as of October 2008) of the law enforcement agencies of the Federal States who comprise the Joint Police and Customs Financial Investigation Groups to combat ML. The Joint Police and Customs Financial Investigation Groups of the 16 *Länder* Bureaus of Criminal Investigation, as specialized departments for financial investigations, act as “clearing offices,” in other words, they review the STRs received and other indications of ML to determine whether liable criminal conduct may be involved. The clearing process and the criminal investigations fall within the original jurisdiction of the Joint Police and Customs Financial Investigation Groups of the Federal States. The Joint Police/Customs Financial Investigation Group of the BKA assists with the clearing process through the prescribed channels, particularly when overseas investigations are necessary.

445. The German Customs Office also plays an important role in the detection and investigation of ML and TF. The Customs Office has 26,000 officers across the country at airports, ports and land-border entry points, as well is in specialized investigative units. There are 43 “Main” Customs Offices across Germany. There are 1,000 customs officers dedicated to Frankfurt (primarily at the international airport there).

446. The Customs Criminological Office based in Cologne has responsibility for customs criminal investigations in the whole country. In 2008, a staff of 3,137 was employed across the entire Customs Investigation Service. Of that figure, 714 were officers working at the Customs Criminological Office and 2,423 were officers working at the customs investigation offices. It has eight local offices in Germany, several of them with specialized responsibilities for the entire country (*e.g.* Hamburg office responsible for investigations at all ports; Essen is responsible for the Dutch border; Frankfurt has responsibility for the airport and all along the French border up to the middle of Germany).

447. ML investigations are embedded in the Organized Crime teams that are dispersed across the country. Customs Investigation officers also work in the Joint Financial Investigation Groups of the 16 states and in the BKA, and in addition to their customs officer powers also have full police investigative powers all over Germany as per Sections 1 (3a) and 12b of the CAA 111a and 12a of the Customs Management Law. Usually they operate under the direction of the state public prosecutor, and in some instances also under the direction of federal public prosecutors.

### **Integrity of Competent Authorities (c. 30.2)**

448. Federal Prosecutors working at the Federal Prosecutors Office in Karlsruhe are carefully screened for entrance. Usually they are recruited from Public Prosecutors from the *Länder*, who have been monitored and trained during a three-year period at the Federal Prosecutors Office.

449. All staff of the Federal Prosecutors Office undergoes an extensive security check. All staff is also subject to a general duty of confidentiality.

450. Police officers at both the federal level and the level of the *Länder* are carefully screened for entrance into police training preparatory to becoming police officers. They are monitored and evaluated during the recruitment and induction period, and their training pays considerable attention to ethics and conduct.

451. All staff of the BKA undergoes extensive security check. All staff of the BKA, including those of the FIU, is also subject to a general duty of confidentiality by virtue of their public office.

452. Within the framework of the training for the police officers within the BKA, and therefore including those of the FIU, ethical fundamentals and integrity training are conveyed in the diploma course of studies as well as within the context of further training which is organized on occasion. Regularly (at least once per year), staff of the BKA receives training on secrecy regulations. In the course of a change-over from a diploma system to a Bachelor course of studies in late 2009, the teaching of basics of professional ethics will be intensified even further through course and training events.

453. With respect to authorities at the *Länder* level, the only information provided relates to screening on recruitment and subsequent law enforcement training.

### **Training for Competent Authorities (c. 30.3)**

454. Employees of the Federal and the *Länder* judicial and law enforcement agencies have access to a comprehensive range of further education and training opportunities.

455. There are various training courses focusing on judicial aspects. The *Deutsche Richterakademie* (German judicial training academy) offers annually specific courses on international legal cooperation in criminal matters. Judges and prosecutors may also attend the courses offered by the European Law Academy. The German EJM contact points meet once a year to discuss matters of common interest. The officials responsible for mutual legal assistance and extradition at federal and state level meet biannually. There are several additional meetings on *Länder* level where appropriate liaison magistrates, foreign officials and the German national Eurojust member take part in those meetings. The German academy offers courses in the English language. Both the German academy and the European academy are open to prosecutors and other officials from other member states. Both institutions regularly invite officials and academics from other member states for presentations and forums. The German academy, with its facilities in Trier and Wustrau, is responsible for the continuing education of public prosecutors. In 2009, various one-week conferences were scheduled on issues relating to ML and related subjects such as:

- Current developments in the law relating to economic crime;
- Organized crime; and
- Current developments in “criminalistics” and criminal justice.

456. Officers recruited to the FIU are assessed on entry, are required to undergo orientation and a basic curriculum in relation to financial crimes and FIU roles and responsibilities, and are encouraged to participate in a variety of financial crimes related training programs available at the BKA, at the *Länder* Police, and in the form of training and continuing education programs offered at the international level.

457. The police also offers various training opportunities. Among the wide range of education and training courses available to the federal and *Länder* employees through the BKA and through *Länder* Police continuing education programs, the following are of direct relevance to ML and TF:

- Financial investigations;
- Introduction to economic crime;
- Advanced course in economic crime (financing offenses, corruption);
- Asset confiscation and recovery;
- Counterfeit currency;
- Narcotics;
- Politically-motivated crime; and
- Proliferation.

458. The 16 *Länder* Bureaus of Criminal Investigation (*Land* or *Länder* Police) also offer comprehensive subject-specific further education and training courses for employees of *Länder* and federal law enforcement agencies (*e.g.* economic crime level 1 to 3 and financial investigations offered by the *Land* Bureau of Investigation in Bavaria). The police education institutions and police academies of the *Länder* also offer relevant training courses (*e.g.* the course in financial investigations offered by the Police Academy of Hesse). *Land* level police officers are also able to avail themselves of many of the training programs offered by the BKA.

459. The Customs agencies also offer training. In principle, only civil servants with several years of experience in the Customs Administration are taken on in the areas responsible for the actual investigations at the Customs Criminological Office and the customs investigation offices. They undergo special training in preparation for their Customs Investigation Service roles. If they require specialized knowledge to carry out their duties (*e.g.* in the area of combating ML), they can attend extra training courses. The Customs Criminological Office holds an annual training course specialized in financial investigations for the staff of the Customs Investigation Service. Besides this, the Customs Investigation Service officers responsible for combating ML also take part in specialist training sessions held by the police. Courses on the topic of asset recovery are offered on an annual basis. These are organized by the Customs Criminological Office for customs investigation officers; for members of the units within customs responsible for controls and prosecution, the federal revenue administration’s training establishment provides the courses.

***Additional Element (Rec. 30) – Special Training for Judges (c. 30.4):***

460. The German Judges' Academy is also responsible for the continuing education of judges (see comments above). The individual *Länder* also offer continuing education courses to their judges.

***Statistics (applying R.32)***

**PRELIMINARY CRIMINAL INVESTIGATIONS AND CHARGES BROUGHT  
BY THE STATE'S PROSECUTION FOR ML (2004–2008)**

	2004	2005	2006	2007	2008	Total
Preliminary investigations initiated	4 770	6 692	9 929	13 593	10 478	<b>45 462</b>
Charges brought	144	129	259	708	766	<b>2 006</b>

***Analysis of Effectiveness***

461. The excellence of the prosecutors from the public prosecution offices of the German *Länder*, of the judges at the courts and the lawyers with the Ministry of Justice, their remarkable knowledge of the law, and their dedication to the responsibility that they have been entrusted with, confirms the solid foundation upon which the German system is established.

462. Despite this major advantage, questions remain about the effectiveness of the process and the difficulties that most prosecutors are finding in investigating and prosecuting ML offenses.

463. According to Sections 160 and 163 of the CPC, it is incumbent on the public prosecutor's office to perform the investigation; in so doing, it may avail itself of officers of the police as persons performing the investigation. In this context, the public prosecutor's office is responsible for supervising, in technical terms, the investigation by the police to ensure this complies with the stipulations of the law; the police officers are under obligation to follow the investigation orders issued by the public prosecutor's office. In order to enable the public prosecutor's office to fulfill its tasks, the police authorities are obliged to enter into contract with the public prosecutor's office from the commencement of the investigation onwards, and must do this all the more so in difficult cases. The public prosecutor's office can then issue the required instructions for further investigation.

464. However, there appears to be a long-time lag between the receipt of an STR by the relevant *Land* police and consideration of the results of the "clearing process." While the prosecutor is technically the "master over preliminary criminal investigations," typically a prosecutor would only see the STR again after the clearing process concludes (which on average usually takes between 3 and 6 months). Unless an urgent need demands it, it is not until the clearing process is completed that the investigation would continue with the use of more "intrusive" probatory measures (such as searches, seizures, or the use of special techniques of investigation described above) and a greater involvement of the prosecutor.

465. For a variety of reasons (mostly described under Recommendation 1), there appear to be relatively few investigations conducted into more complex ML structures, where professional money launderers may be acting separately from the persons involved in the commission of the predicate offense, which is often the *modus operandi* for organized crime. This is consistent with the authorities' indication that more emphasis could be placed in prosecuting serious ML as an effective tool to tackle serious crime (more attention being given to the investigation and prosecution of predicate crimes).

466. LEAs may also obtain information from the BaFin's automated account access system about bank accounts (see more information in section 7.2 below). When making an inquiry to the BaFin

regarding the automated account access system, LEAs do not have to name the type of offense underlying their investigation. However, occasionally law enforcement agencies do name the underlying offense, and ML and TF have been named in this context. Hence, the BaFin is able to confirm that the automated account access system is used by law enforcement agencies in ML and TF investigations, but is not able to provide statistics or even estimates on the number of such investigations.

467. The authorities also confirmed that some of the more intrusive special techniques of investigation are only being used to investigate serious offenses. Accordingly, as ML is categorized as a “less serious offense” not much use is being made of some of these special investigation techniques to investigate ML offenses.

468. Finally, some prosecutors indicated that there appears to be a greater degree of success in achieving indictments for ML conducts in jurisdictions where the prosecution offices pursue these type of investigations through sustained specialized units (both at the law enforcement and prosecutor levels). It may, therefore, be useful to give more consideration to proposals aimed at spreading the concept of specialization for the investigation of financial crimes across all jurisdictions.

469. The authorities did not provide statistics on ML investigations or TF investigations and prosecutions, nor on the use of special investigative techniques or other investigative powers. It the absence of such statistics, it was not possible to fully assess the effective implementation of Recommendations 27 and 28.

### 2.6.2. Recommendations and Comments

470. In order to comply fully with Recommendation 27, Germany should:

- Make more use of special techniques when conducting investigations into ML.
- Undertake actions (awareness raising or training) to improve the focus of ML investigations and the amount of investigations conducted into more complex organized crime ML structures.

471. In order to comply with Recommendation 28, Germany should:

- Maintain complete statistics on the use of powers to conduct ML or TF investigations and prosecutions.

### 2.6.3 Compliance with Recommendations 27 & 28

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
R.27	LC	<ul style="list-style-type: none"> <li>• The offense of ML is not being properly investigated. The focus is placed on self launderers with few investigations conducted into more complex organized ML structures.</li> <li>• The lack of complete statistics has prevented assessors from fully evaluating the effectiveness of this recommendation.</li> </ul>
R.28	LC	<ul style="list-style-type: none"> <li>• The lack of complete statistics has prevented assessors from fully evaluating the effectiveness of this recommendation.</li> </ul>



## 2.7. Cross-Border Declaration or Disclosure (SR.IX)<sup>54</sup>

### 2.7.1. Description and Analysis

#### *Legal Framework:*

472. Germany has two different legal requirements in place to monitor cross-border physical transportation of currency and negotiable instruments; one applies to movements between Germany and non-EU countries and entails a declaration obligation (a), the other applies to movements within the EU and carries a disclosure obligation (b).

- a. EU Regulation 1889/2005 on controls of cash entering or leaving the community applies to controls at the Community's external borders (*e.g.* borders between Germany and Switzerland, or persons entering Germany from or departing for a non-EU country by air). Authorities state that it is directly applicable in Germany. It requires that all travelers crossing the EU's external frontiers complete a written declaration if they are transporting EUR 10 000 (USD 13 917) or more in "cash." Article 2 of the Regulation defines cash as including currency and bearer negotiable instruments that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such a form that title thereto passes on delivery, as well as incomplete instruments (such as promissory notes and money orders) signed but with the payee's name omitted. Article 12a of the CAA requires that the declaration be made in writing on entering or leaving the EU territory.
- b. With respect to borders with other EU member states, Sections 1 and 12(a) of the CAA provides that "the movement of cash or equivalent means of payment" in excess of EUR 10 000 are subject to monitoring by the authorities "into, out of, and through the area of application" of the Act. Travelers are required to make an oral disclosure when asked by a Customs officer. The authorities state that there is no differential treatment of funds moving from or to Schengen Zone countries<sup>55</sup>. The decisive issue is whether currency and negotiable instruments are moving between Germany and non-EU countries (in which case EU Regulation 1889/2005 applies) or within the EU (in which the CAA applies).

473. German authorities state that the term "equivalent means of payment" (as set out in Art. 1(3a) (sentence 4) of the CAA, in conjunction with Art. 1(1) of the German Securities Deposit Act) corresponds with the FATF definition of "bearer negotiable instruments," and also includes "electronic money."

<sup>54</sup> This assessment was conducted on the basis of the requirements in place at the borders into and out of Germany. FATF agreed in February 2009 that a supra-national approach could be applied for EU countries. However, the supra-national approach has not been used to rate this assessment at the request of the authorities and also because further discussions are needed about how to implement a supra-national assessment. Nonetheless, the measures that Germany has in place that relate to the supra-national approach have been taken into account to the extent that they are relevant.

<sup>55</sup> The countries comprise: Austria, Belgium, Czech Republic, Denmark (excluding Greenland and Faroe Islands); Estonia, Finland, France (including Monaco, but excluding all overseas departments and territories); Germany, Greece (excluding Mount Athos), Hungary, Iceland, Ireland (police and judicial cooperation only); Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands (excluding Aruba and Netherlands Antilles), Norway (excluding Svalbard), Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom (police and judicial cooperation only - including Gibraltar but excluding Guernsey, Isle of Man, Jersey and all overseas territories outside of Europe). In addition, the following countries have opted into the zone but have yet to implement the requirements to be full members: Bulgaria, Cyprus, Liechtenstein and Romania.



Documents not falling within “equivalent means of payment” may nevertheless be seized or restrained if a specific suspicion of ML/TF arises. With regard to suspected ML, specific reference to this authority is made in paragraph 33 of the “Service Regulation pertaining to the implementation of Regulation (EC) No. 1889/2005 of the European Parliament and of the Council of October 26, 2005 on controls of cash entering or leaving the Community”. In the case of suspected TF, explicit reference is made in paragraphs 36 and 40 of the Service Regulation, in conjunction with Sections 129(a) and 129(b) of the CC and Sections 94 and 98(1) of the CPC.

***Mechanisms to Monitor Cross-border Physical Transportation of Currency (c. IX.1):***

474. As mentioned above, travelers crossing the EU’s external frontiers are required to make a written declaration if they are transporting more than EUR 10 000 (USD 13 917) in currency or specified negotiable instruments. The authorities state that extensive measures have been taken to implement the declaration requirement. They indicate that posters, signs, and brochures are deployed at land and sea borders and, to varying degrees, also at airports, informing travelers of the requirement to make a declaration.

475. Assessors observed, however, that implementation at airports of the declaration requirement for travelers is variable and problematic for incoming passengers. Authorities acknowledged that arriving air passengers are not supplied with a declaration form prior to landing, and are not otherwise advised prior to arrival of their obligation to make a declaration. Notices to travelers about the requirement are posted in some airports, but in the airport visited by assessors, they were not particularly conspicuous to travelers finding their way through the airport terminal, confronted by a myriad of commercial and noncommercial signs and posters. Declaration forms are reportedly available in the Customs area, but were not readily visible to assessors. Travelers are not automatically required to present a declaration form along with their travel documents when passing through the first entry points.

476. At airports, after collecting their luggage, travelers can pass through the “Green” lane which is not staffed, or can choose to pass through a “Red” lane where they make declarations, including declarations regarding the import of currency and negotiable instruments. While the “Green” lane is not “staffed” as such, it is monitored and attended by customs officers whose purpose is to check for passengers who have made a written currency declaration. Passengers who choose the “Red” lane are subject to inspection and can be, and frequently are, asked by Customs officers whether they wish to make a disclosure in respect of currency or negotiable instruments in excess of the reporting threshold. Following a disclosure, baggage is routinely inspected to verify the amounts and types of currency and instruments being transported, as well as to collect information to assist in the validation of profiles.

477. Section 10 (1), of the CAA (on the right to stop persons and vehicles) permits persons and vehicles to be stopped for the purposes of cash controls to perform the tasks identified in Section 1(3a) of the CAA in conjunction with Section 12 a (3), of the CAA, at areas near to the EU’s external borders (Section 14(1) of the CAA). The same applies to areas near to the internal EU borders (Section 12 a (3), of the CAA).

478. Travelers can be stopped by Customs officers at ports of entry or elsewhere and asked to make a verbal disclosure as to the amount, source, beneficial ownership and intended purpose of any currency or instruments they carry in excess of the EUR 10 000 (USD 13 917) threshold. Requests for disclosures are made based on the experience of the Customs officer, and are not required to be based on suspicion. Controls specifically targeting movements of currency and negotiable instruments take place at the border (pursuant to section 12 (a) of the CAA) or within 30 km of the border pursuant to Section 14 of the CAA.

479. Under Section 12a(3), and Section 10(2) of the CAA, the powers in Section 10(1), of the CAA (on the right to stop persons and vehicles) also apply within the **national territory** (beyond the border areas) for the purposes of performing the tasks named in Section 1(3a) of the CAA if there is reason to believe that means of payment subject to customs supervision under the CAA, the “Service regulation pertaining to the implementation of Regulation (EC) No. 1889/2005 of the European Parliament and of the Council of October 26, 2005 on controls of cash entering or leaving the Community” and the Service Regulation on the Monitoring of Cross-Border Cash Movements, are being carried by persons.

480. Customs monitors the intra-EU flow of goods and currency. Persons and vehicles can be and are stopped and checked anywhere in Germany, pursuant to Section 10(2) of the CAA. The checks cover a variety of goods and items within the Customs mandate, including currency, bonds, dividend coupons, investment fund certificates, checks, bills of exchange, precious metals, precious stones, and electronic money. Checks are conducted at random, and are not required to be based on suspicion. Persons stopped for such checks may be asked to make a disclosure of currency or equivalent means of payment being transported that are above the threshold, and their luggage, vehicles and persons may be examined to verify the accuracy of the disclosure.

481. Customs powers to inspect intra-community cash movements are regulated by the CAA and an implementing Service Regulation on the Monitoring of Cross-Border Cash Movements. Section 10(2) of the CAA permits customs controls to be conducted throughout the entire country. The basic requirement for conducting a cash control within the national territory is reason to believe that the border has been or will be crossed and that goods and cash subject to Customs supervision are being transported. Specific detailed rules concerning intra-community cash movements are also established as required – over and above the powers noted above – through internal administrative instructions, such as orders from the Federal Ministry of Finance or from Federal Finance Offices.

482. Mail, courier, and cargo shipments, both incoming and outgoing, are also subject to inspection for transport of currency and negotiable instruments. Section 10(4) of the CAA authorizes Customs employees to open and check consignments which are presented to them. Cargo shipments are subject to a risk-based inspection system for air and sea cargo, including x-ray inspection. Mail or courier shipments are less amenable to risk-based inspection and therefore about 85–90% of such shipments are subject to x-ray and other forms of inspection. The authorities were unable to confirm whether mail and courier shipments are subject to a legal requirement for a written declaration as to the contents, and if so, whether that is made at the time each mail or courier package is handed over to the post office or courier company.

483. All postal consignments entering or sent from the European Community are subject to customs supervision (Section 1(3a) and 10(1) and (2) of the CAA). Section 10(5) indicates that privacy of correspondence and posts are restricted in relation to Customs supervision carried out under Section 10.

484. As a part of this supervision, Customs inspects, for example, whether import duties are to be paid for the postal consignments, whether the postal consignments contain goods subject to prohibitions and restrictions, and whether all of the information and documents required for the postal consignment are complete. It is also important that the customs officers know exactly what a package contains. The description of contents on the customs declaration affixed to the postal consignment, or in other documents, is often not sufficient to assess the contents. For this reason, the customs authorities may have consignments that are transported by post opened by Deutsche Post AG so that customs officers can check the contents (Section 10(4) of the CAA). The privacy of correspondence and post is restricted in this respect (Section 10(5) of the CAA).

485. Postal consignments from countries within the customs territory of the European Community are not generally dealt with by the German Customs Administration because these consignments are being

transported within the single market and thus fall under the free movement of goods. In certain situations, postal consignments transported within the EU may, however, be inspected. In line with Section 5(1) of the CAA, Deutsche Post AG is to present consignments to the customs authorities for further inspection where there are sufficient factual indications showing that the consignments contain goods whose importation, transit, or exportation breaches statutory prohibitions and restrictions. These consignments may also be opened and the contents inspected.

486. If investigations by the Customs Investigation Service or conspicuous features otherwise determined substantiate indications of an offense (*e.g.* TF under Sections 129(a) and 129(b) of the CC), the customs authorities and customs investigation officers, in particular – as investigators of the public prosecutor’s office – are authorized to present the goods in question to the public prosecutor’s office for subsequent prosecution and for the public prosecutor’s office to take a decision on attaching the consignment (Sections 99 and 100 of the CPC). This also applies to postal consignments transported by courier services or transport or logistic companies other than Deutsche Post AG.

487. With respect to cash controls in connection with the carriage of passengers on cruise ships and ferries, and checks on crews, there is a distinction drawn between passing vessels and anchoring vessels (Article 52 of the Convention on the Law of the Sea) as applied to the inspection of commercial ships on the North Sea and Baltic Sea. Passing vessels are questioned via radio about port of departure, port of destination, and their cargo. Data are verified with the help of the coast guard. If this gives rise to a reasonable suspicion (based on risk related to route, country of origin, nationality of passengers, etc), the ships are directed to a port for further questioning and customs inspection as applies to all anchoring vessels. In the case of private maritime traffic, controls pay particular attention to the crew and passengers.

488. As concerns the operation of ferries on Lake Constance (bounded by Germany, Austria, and Switzerland), passengers are inspected on a random basis when disembarking. The crew is not subject to controls. Authorities indicated that controls cannot be conducted on Lake Constance itself because the national territory is not defined.

### ***Request Information on Origin and Use of Currency (c. IX.2)***

489. Pursuant to Section 12(a) of the CAA, declarations of movements of currency, or bearer negotiable instruments, or both, from or to non-EU member states are required to be made in writing. If asked by a Customs official, travelers have to provide information such as the source, name of the beneficial owner and intended use of the currency or specified instruments. (The authorities were unable to clarify which definition of beneficial owner is applied in this situation.)

490. Similarly, pursuant to Section 1 and 12(a) of the CAA, travelers from or to EU member states may be requested to make oral disclosures, and they too have to provide information as to the source, beneficial owner and intended use of the currency or specified instruments if asked by the enquiring customs officer. German customs officials have the authority to request such information, including in cases where false or misleading declarations or disclosures have been discovered or when no declaration has been made.

### ***Restraint of Currency (c. IX.3)***

491. Section 12 a (4) and (4a) of the CAA provide that, if there is reason to assume that cash or equivalent means of payment are being transported for the purpose of ML or TF, customs officers may restrain the cash or the equivalent means of payment and take it into custody for up to three working days to clarify the source and intended purpose of the funds. Based on a court order of the county court in whose jurisdiction the restraint took place, the measure may be extended up to a month. Law enforcement

authorities have to be informed immediately of any restraint carried out by the Customs authorities. Undeclared cash that is discovered, but which is not suspected of being related to ML or TF, is subject to administrative fines up to EUR 1 million (USD 1.4 million) (Section 31a).

492. The authorities indicate that customs officials on site may decide, without any specified or defined suspicions, to conduct a search and restrain funds. There are no set criteria, and subjective criteria such as the travelers' appearance and demeanor, the experience of the customs officer, etc. play a role. The provision of false information about the amount or means of payment being carried may in itself constitute an indication of ML or TF and may lead to the restraint of funds for the purpose of clarifying the matter. Customs officials indicated that all funds, not simply those amounts above the reporting threshold, can be restrained. These measures apply to the movement of funds across EU borders as well as to intra EU movements or shipments.

***Retention of Information of Currency and Identification Data by Authorities when appropriate (c. IX.4)***

493. Pursuant to Section 12a (5) of the CAA, the German customs authorities have legal authority to collect, process and use all the data gathered from the declaration or disclosure requirements, including information or data in relation to false declarations or disclosures failure to make a declaration or where there is a suspicion of ML or TF. The authorities can also share such information with the law enforcement and other competent authorities. Reports and other data are entered into the Customs database, INZOLL, which is accessible, in practice, to Customs officers, the Customs Criminal Investigation Service, some *Länder* LEAs, and the BKA, including the FIU.

494. The data are stored for one year, using a special protected access category. The paper declarations are also destroyed after one year. If criminal investigation(s) take place, the data can be retained for longer than one year. This short retention period considerably diminishes the utility of the database for analytic purposes.

495. There is a comprehensive process in place for recording the relevant information and a number of standard forms that customs officers use to record the information received from declarations or disclosures and forward it for entry into the INZOLL database. The following are examples of such forms:

- Form No. 033008 "Control Report".
- Form No. 0402 "Cash Control with Follow-Up Measures".
- Form No. 0405 "Cash Control without Follow-Up Measures".

496. These forms are used to collect information about: identity (of the officer conducting the control and the persons subject to the control); customs office; place, time and reason for control; means of transport; route; results of questioning regarding the transportation of cash, information about how the cash is split, place where cash is found, currencies, total amounts; discrepancies between traveler's response to first and second round of questions; control measures such as seizure, imposition of the provision of collateral, initiation of administrative fine proceedings; transmission of data to authority relevant in light of the findings.

497. Once the controls are complete, the customs officers send the completed forms to the relevant unit (determined on the basis of the findings) responsible for processing the matter further. This could be such units as the main customs offices, the cash declarations unit at Hanover main customs office (this is the unit responsible for entering data into INZOLL) or the BaFin, the Customs Criminological Office,

customs investigation office or other revenue authority of the *Länder*. This is where the control reports are entered into the relevant database and processed further.

***Access to Information by FIU (c. IX.5)***

498. Information about declarations, seizures, fines and other measures, including any ensuing criminal investigations, is entered by Customs into the INZOLL database which can be accessed by the FIU for the purposes of analysis of STRs. The *Länder*-level investigative authorities, the Joint Financial Investigations Groups, include the presence of Customs investigations officers who have direct access to the INZOLL database. As noted above, the one-year period of retention of most data in the INZOLL database considerably diminishes the utility of that database for analysis by the FIU and other agencies.

***Domestic Cooperation between Customs, Immigration and Related Authorities (c. IX.6)***

499. Cooperation and coordination among *Länder* and BKA and customs and related authorities in matters related to ML and terrorism financing has been well established for more than 10 years. This has been achieved through a high level of shared investigations, and the development of inter-authority agreements between the Customs investigation services and police bodies at the federal and state levels, as well as between the customs office and police at the local level. In addition, there is institutionalized cooperation in the Joint Investigation Groups which are jointly staffed by *Länder* criminal police and the Customs Criminal Investigation Office personnel, as well as staff from other investigative bodies, bringing together experts in investigations of banking and financial transactions in relation to combating ML. Among other cases, all of the cases arising from the border and inland cash control initiatives are investigated in these Joint Investigation Groups

***International Cooperation between Competent Authorities relating to Cross-border Physical Transportation of Currency (c. IX.7)***

500. Articles 6 and 7 of EC Regulation No. 1889/2005 allow for the exchange of information with other EU member states and non-EU member states. Article 6 applies to the exchange of information between EU member states and allows for the transmission of information gathered through the declaration or disclosure process when there are indications that the sums of cash are related to any illegal activities associated with the movement of cash. As a member of the EU, Germany also applies EC Regulation 515/97 on mutual assistance in customs matters. Article 7 (above) further provides for the exchange of information with non-EU member States upon certain conditions.

501. Furthermore, Section 11 of the CAA, which applies to data and information gathered under the declaration or disclosure process, permits the German customs authority to “transmit personal data to foreign customs, police, judicial and administrative authorities as well as to other foreign public authorities responsible for the prevention or prosecution of crimes, if such information is necessary (1) for the fulfillment of a task incumbent upon them according to [the CAA] (2) for the prosecution of crimes [...] or for the averting of grave danger to the public safety.” A federal court has determined information is “necessary” if the foreign authority needs it to complete its case.

502. With regard to cooperation with third countries, German Customs authorities consider in the specific case at hand whether the existing international agreements on mutual assistance in the field of customs permit cooperation between customs administrations for the purpose of combating ML. This would be applicable where the alleged crime of ML is not investigated in isolation, but in connection with customs offenses.



503. To combat ML, the Customs Administration (Customs Investigation Service) furthermore cooperates with the competent authorities of other states on the basis of the following:

- Government agreements between the police administrations, which also encompass the Customs Administration to a large extent, to combat organized crime.
- Europol Convention.
- Instructions from the public prosecutor's office in the framework of judicial legal assistance.

504. An administrative provision from the Federal Ministry of Finance instructs the customs offices to inform the Customs Criminological Office immediately about information that they believe should be forwarded to other member states. As the central body for legal and administrative assistance in customs matters, the Customs Criminological Office examines the extent to which it is permissible to transfer the data to the other member states and instigates the transfer of the necessary information on the basis of the available legal framework.

505. The Customs Criminological Office must also be informed of transactions that may be of interest to third countries. The Customs Criminological Office examines whether the legal and practical conditions to exchange information are in place and then initiates the necessary steps.

506. In addition to the exchange of personal data, general findings associated with the cross-border transportation of cash are exchanged where this may be important for the other state's administration. This general information includes, *e.g.* notifications about places of concealment or other special characteristics identified in cash controls that are made available, among others, to the World Customs Organization (Regional Intelligence Liaison Office for Western Europe) and the foreign customs liaison officers accredited in Germany as well as the liaison officers of the Customs Criminological Office that are deployed abroad. This is done to enhance the exchange of information further.

***Sanctions for Making False Declarations / Disclosures (applying c. 17.1-17.4 in R.17, c. IX.8)***

507. Noncompliance with the obligations to declare or to truthfully disclose cross-border cash transactions constitute administrative offenses, sanctionable pursuant to Articles 31a and 31b of the CAA. The penalty available is a fine of up to EUR 1 million (USD 1.4 million). The competent authority to apply the sanction is the main local customs office.

508. As set out in internal administrative instructions, the amount of the fines depends on the amount of the undeclared means of payment. The factual circumstances must also be taken into account when setting the fines. In particularly severe cases, the amount of the administrative fine may be set at the amount or value of the cash that the traveler failed to declare or disclose or did not declare or disclose in full.

509. In the field of administrative offenses, authorized representative bodies (Section 30 (1) of the Administrative Offenses Act) of enterprises, investment companies, tax consulting or accounting firms, or other companies — active in the financial services sector — can be held liable for the administrative offenses they or their subordinates commit. This means that insofar as they are equipped with legal powers of attorney, the authorized representative bodies — *i.e.* chairpersons of the supervisory board, management boards, owners, persons with power of attorney, senior management — are either held liable for their own actions (with penalties under Sections 9(1) number 1, 10, 17 and 30(1) of the Administrative Offenses Act) or, by means of Section 130 of the Administrative Offenses Act, the action of subordinates bound by their instructions is attributed to them (with penalties under Section 130 of the Administrative Offenses Act in

conjunction with Sections 9 (1) number 1, 10, 17 and 30 (1) of the Administrative Offenses Act). In Germany, the latter is dealt with under the breach of duties of supervision, which applies to managers and is referred to as directors' and officers' liability. This is subject to the principle that management, as an expression of its elevated position, is responsible for the activities of its employees.

510. Administrative fines for failing to declare or making false declarations or disclosures are used quite extensively, though the fines, in the aggregate amounted to less than 10% of the undeclared funds. In 2007, there were 265 administrative fines levied by Customs for reporting violations, involving EUR 14.7 million (USD 20.5 million), with fines of just over EUR 1 million (USD 1.4 million). Of the 265 cases, 42 were recorded as "intentional" and 23 as negligent. In 2006, there were fines of EUR 1 275 million (USD 1.8 million) levied in 272 cases. In 2008, owing to some organizational changes and changes in the way in which data were collected and recorded, the numbers are not directly comparable to 2007. However, Customs reports indicate that there were 663 cases of undeclared cash or equivalents (160 intentional and 513 found to be negligent). There were 673 fines levied valued at EUR 1 485 million (USD 2.1 million) against EUR 17.3 million (USD 24.1 million) being transported. In the period 2005–2008, there were 197 ML investigations processed on the basis of funds detected during cash controls. Only one of those resulted in a conviction for ML.

#### **Investigations by the public prosecutor triggered by cash controls**

Year	2005	2006	2007	2008
<b>Quantity</b>	53	37	62	45

#### ***Sanctions for Cross-border Physical Transportation of Currency for Purposes of ML or TF (applying c. 17.1-17.4 in R.17, c. IX.9)***

511. Section 12a(4) of the CAA provides that if there is reason to assume that cash or equivalent means are being transported for purposes of ML or TF Customs officers may seize or restrain the cash or equivalent means and take it into custody. Law enforcement authorities are notified immediately and investigations ensue.

512. In 2007, there were 136 instances of cash or equivalent means being detected as possibly connected to ML (75 on entry and 61 on exit) and 11 cases with indications of financing of terrorism. In 86 of these 147 cases, the cash being transported was seized and taken into Customs custody.

#### ***Confiscation of Currency Related to ML/TF (applying c. 3.1-3.6 in R.3, c. IX.10)***

513. As outlined above, Sections 12a (4) and (4a) of the CAA allow for the application of seizure if there is reason to suspect that cash or equivalent means of payment are being transported for the purpose of ML or TF to clarify the source and intended purpose of the funds.

514. Confiscation pursuant to Sections 73 and 74 of the CC can be applied if it can be proved that the money or bearer negotiable instruments are proceeds obtained from the commission of any predicate, ML, or terrorism financing offense.

#### ***Confiscation of Currency Pursuant to UN SCRs (applying c. III.1-III.10 in SR III, c. IX.11)***

515. Funds and assets of persons and entities that are used for TF are frozen according to EC Regulation No. 881/2002 of May 27, 2002 and EC Regulation No. 2580/2001 of December 27, 2001. The assessors were unable to establish whether Customs has access to the lists made pursuant to



UNSCR 1267/881 and UNSCR 1373/2580 and Article 6 of the Banking Law, and, if so, how they get these lists, or how they apply them at the border.

***Notification of Foreign Agency of Unusual Movement of Precious Metal and Stones (c. IX.12)***

516. Within the EC, the reporting of cash and other means covers precious metals and stones. That is not the case for controls at the EC external frontiers. However, a customs declaration is required in any event when these goods are imported even if their value does not exceed the threshold value. Where there is a link to ML or terrorism financing, information is exchanged with other countries under conditions set out in IX.7. Customs officials reported that there had been information provided by Germany to three foreign jurisdictions (Canada, Israel and Mexico) about significant discoveries of precious metals and stones.

***Safeguards for Proper Use of Information (c. IX.13)***

517. Authorities state that Customs internal administrative instructions require that cash declarations must first be recorded centrally at the main customs office in Hanover, before those data are entered in INZOLL. Inspections conducted by the data protection authority with local jurisdiction ensure that data protection is observed with regard to sensitive personal information. The administrative instructions for employees of the cash declaration unit are also subject to review in terms of data protection. Requirements for the protection of data apply also to intra-community movements, which includes the information obtained through oral disclosures. Every authority involved has its own (local) data protection officer.

***Training, Data Collection, Enforcement and Targeting Programs (c. IX.14)***

518. Extensive training is provided to Customs Officers to equip them to carry out their assigned functions. This includes introductory and advanced courses on monitoring of cross border cash movements and covers topics such as main tasks and competences, object of inspections, powers of inspection including the limits on those powers, principle of mandatory prosecution, provisions of limiting powers, application of force, rights in exceptional circumstances. There is also practical training for purpose of carrying out controls and monitoring, including procedures for controls, procedures to be applied for indications of ML or suspicions of ML. There is further training in conducting administrative fine procedures.

519. In addition to training on powers and procedures, specific training is also provided on: the obligations of travelers; searching of personal baggage and vehicles; follow-up measures to indications or suspicions of ML or terrorism financing; seizure of cash and, equivalent means of payment, or both; reporting channels, and, cooperation with German police and the Customs Investigation Service. The Customs Criminal Office holds annual training courses specialized in financial investigations for the staff of the Customs Investigation Service. In addition, courses on asset recovery are also offered on an annual basis.

***Supra-National Approach: Timely Access to Information (c. IX.15)***

520. N/A.

***Additional Element – Implementation of SR.IX Best Practices (c. IX.16)***

521. Germany applies a EUR 10 000 (USD 13 917) threshold for reporting of cross-border movement of currency and bearer negotiable instruments. To detect potential false declarations or disclosures and possible ML and TF, the competent officers carry out controls. The controls are normally performed on a risk-based approach, although some targeted checks are performed as well. The customs officials

monitoring cross-border cash movements are provided with the knowledge and information they require to complete their tasks in multi-regional training and educational courses. They are also regularly provided with practical cash information updates, which contain case-specific information *e.g.* about possible methods of concealment. Furthermore, x-ray machines, both mobile and stationary, are used in controls, particularly at airports, but also on the roads. Germany has seven specially-trained cash detection dogs.

522. When suspicious currency and bearer negotiable instruments are detected, the luggage is kept in a special room for examination, paperwork, and securing the evidence. Usually, photos are taken. The seized cash and bearer negotiable instruments are deposited in an evidence room, which is part of every customs office.

523. Germany continues to have high-denomination banknotes (EUR 500 = USD 696) in circulation. In 2008, according to the “Situational Analysis” report for that year, in 267 “clearing operations” (initial investigations) cases for which information on denominations of banknotes was available, all involved a preponderance of EUR 500 banknotes, and 49 of those cases involved persons carrying exclusively EUR 500 banknotes.

#### ***Additional Element – Computerization of Database and Accessible to Competent Authorities (c. IX.17)***

524. Reports and related information are entered in INZOLL and the information is readily accessible, in practice, to Customs officers, some *Länder*, the BKA (including the FIU) and to prosecutors. Customs officers in Joint Financial Investigation units have direct access to the database. The FIU also has access to this database. The fact that significant portions of the data are only stored for one year, and the paper declarations are also destroyed after one year (unless subject to criminal investigation) is a pronounced shortcoming of the database in terms of its utility for identifying cash couriers, or identifying trends or typologies.

#### ***Statistics (R. 32)***

525. Customs Administration (and the Customs Investigation Service) collects and maintains a broad range of statistics about cross-border transportation of currency and instruments, restraints, investigations, seizures and confiscations. This information is available to other agencies with responsibilities for AML/CFT. Much of it is also analyzed and published in various publications of the Customs service. The Customs Investigative Service, for example, has published, among other documents, an annual “Situational Analysis relating to the monitoring of cross-border cash movements.” The Federal Finance Office Southeast (the Central Unit on Cash Movements) in 2008 took on the responsibility of producing and publishing a consolidated study.

526. Both of these reports contain a wide range of annual and multi-year data about all aspects of cross-border movements of cash and equivalents. These are displayed geographically (by region) and functionally (by the type of control point, *i.e.*, airports, roads, rail, and sea), by type of currency, whether on entry or exit. Also reported are the number and scope of “clearing operations” conducted, the amount of money that was being transported in those cases as well as the currency denominations, differentiated as to “intra-community” or “third country,” the number of investigations triggered by cash controls, number of convictions, cases abandoned, and value of cash or equivalents permanently confiscated.

#### ***Adequacy of Resources – Customs (R. 30)***

527. Germany’s Customs Administration and Customs Investigation Service appear to be adequately resourced.

528. The Customs Administration has 34,102 officers across the country at airports, ports and land border entry points, as well as in specialized investigative units. There are 43 “Main” Customs Offices across Germany.

529. There are 1 000 customs officers dedicated to Frankfurt (primarily at the international airport there).

530. The Customs Criminological Office is based in Cologne, with a staff of 714, and has responsibility for customs criminal investigations in the whole country. It has 8 local offices in Germany (with a combined staff of 2,433), and several of those offices have specialized responsibilities for the entire country (*e.g.* Hamburg office responsible for investigations at all ports; Essen is responsible for the Dutch border; Frankfurt has responsibility for the airport and nearly all along the French border up to the middle of Germany).

531. ML investigations are embedded in the Organized Crime teams that are dispersed across the country. Customs investigation officers also work in the Joint Financial Investigation Units of the 16 states, and, in addition to their customs officer powers, also have full police investigative powers all over Germany as per Sections 1(3)a and 12b of the CAA. Usually they operate under the direction of the *Länder* public prosecutor, and in some instances also under the direction of federal public prosecutors.

### ***Special Case of the Enclave of Büsingen***

532. Under Article 3 (1), fifth indent of Regulation (EC) No. 450/2008 of April 23, 2008 laying down the Community Customs Code (Modernized Customs Code), Büsingen is not part of the EU’s customs territory. There are various special rules because, while it is a German exclave, it also belongs to the Swiss customs territory:

533. On October 4, 1967, a bilateral customs agreement entered into force as a result of German-Swiss negotiations. Under this treaty, the police of the Canton of Schaffhausen may autonomously carry out arrests in the territory of Büsingen and move the arrestees into Switzerland. The number of Swiss police officers that are allowed to be present in Büsingen at the same time is limited to 10. The number of German officers is set at three per every 100 inhabitants. The competencies of the Swiss police lie in the fields in which Swiss laws apply (*e.g.* in the areas of customs, agriculture, and the hotel and restaurant industry, etc.). German customs officers do not, therefore, have any powers whatsoever in Büsingen.

534. The first German customs control point is the Gailingen-West customs office. This customs office is located on the only road leaving Büsingen and leading to Germany via Swiss territory. Travelers are subjected to controls (including cash controls) here on a daily basis. Seizures in the last three years have concerned cases of capital flight only. No seizures in the field of ML or TF were registered.

535. Apart from a few exceptions, Swiss customs and commercial law applies in Büsingen. The direct taxes of the people of Büsingen (*e.g.* income tax) must be paid over to the German revenue authorities.

536. German authorities indicate that, according to their information, banks in the international financial sector do not play a significant role in the 2 000–3 000 strong territory of Büsingen and that taking into account points noted above, Büsingen has not so far become conspicuous for ML or TF crimes.

### ***Analysis of Effectiveness***

537. As noted above, the Customs Administration has responsibility for administering the law and regulations relative to the cross-border movement of currency and negotiable instruments. The Customs Criminal Investigation Office has the responsibility and powers to investigate violations.

538. The Customs Administration is a robust organization, with some 34 102 officers in the country, with responsibility for 71 land border-crossing points (road and rail), 23 international airports, and 25 maritime ports (with international maritime traffic). Some 1 000 officers are assigned to Frankfurt airport, the main international airport in the country.

539. The Customs Investigation Office has 2 433 officers spread over eight offices in Germany, each office having both general and specialized functions.

540. The Customs Administration has broad powers to carry out its functions. There appears to be a well developed risk-based approach to the entire mission, focusing on the higher-risk geographic areas, as well as higher-risk activities and functions in those areas. The border controls are buttressed by ready access to intelligence information from the INZOLL database and technical inspection technologies. At Frankfurt airport, in addition to static customs points, there is a cash control unit of 15 officers that check incoming and outgoing flights on a risk-assessed basis. On high-risk flights, as many as two-thirds of passengers are checked, in part, to validate the profiles that have been developed and are continuously updated. Last year, the cash control unit seized some EUR 35 million (USD 49 million) at the airport that had been undeclared and identified about EUR 100 million (USD 140 million) in legally-declared currency and instruments being transported by travelers.

541. In addition to the stationary controls at ports of entry and exit, there are some 1 600 officers assigned to roving inland control teams that check travelers in border areas, as well as (somewhat surprisingly) much farther inland. Their powers (noted above) permit them to stop travelers without first having to establish suspicion, and they can enquire about and search for any goods and contraband, as well as for currency and negotiable instruments. As is the case at border points, when undeclared or falsely declared or disclosed or suspicious funds are found, they can be restrained. There is a fast-track process for clarifying the facts on the spot by the customs officer. If that does not resolve the suspicion, funds can be seized and the investigative process initiated by an immediate report to the competent authority.

542. As already noted, mail, courier and cargo shipments are also subject to controls. The authorities state that some 85–90% of mail and courier shipments are checked. Freight shipments are also checked on risk-based assessment and inspection of shipping documents and through physical and technical searches. Sea cargo is also subjected to document inspection, buttressed by x-ray inspection on a risk-assessed basis.

543. Notwithstanding the very positive assessment of the overall Customs initiative in respect of SR.IX, assessors must highlight a noticeable weakness in the system of obtaining declarations from travelers at EU borders of German international airports. Forms for travelers' declarations are not distributed to travelers before arrival. Nor are they always readily visible at counters approaching the customs point. Assessors were informed that there are signs placed in entry points to the terminal and in approaches to Customs points, alerting travelers to the currency and instruments declaration requirement. When those signs were shown to assessors at Frankfurt Airport it was difficult to distinguish them from a number of similar looking signs advertising products and services available within the terminal. In addition, assessors did not notice any signage when arriving in Germany at other airports from the one at which the assessors were shown the signs.

544. The authorities note that arrangements for displaying information notices alerting arriving passengers have to be worked out with individual airports and that there is no power to impose specific requirements. Some airports, such as Stuttgart, are cited as models, and some others are also quite cooperative and helpful, while some others may be less inclined to go out of their way to assist in the communications task.

545. Assessors were not in a position to view at first-hand the effectiveness of the implementation of the declaration and disclosure processes that apply at land and sea ports. Nonetheless, given that the EU has largely eliminated border posts between member states, and based on assessors' general experience of crossing land borders between EU nations, it is highly likely that there are many land border crossings where there is no effective scrutiny to require disclosures.

546. Assessors did see evidence that passengers departing the EU from German airports are alerted to the declaration requirement at check-in via LCD screens.

### **2.7.2. Recommendations and Comments**

547. In order to comply fully with SR.IX, Germany should:

- Take steps to heighten arriving and departing travelers' awareness of the declaration and disclosure requirements by making much more visible (and perhaps in multiple languages) the signage at ports of entry and exit alerting travelers to the requirement.
- Extend the one-year period of retention of most data in the INZOLL database.

### **2.7.3 Compliance with Special Recommendation IX**

	<b>Rating</b>	<b>Summary of factors relevant to s. 2.7 underlying overall rating</b>
<b>SR.IX</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Weakness in measures for alerting air travelers arriving in Germany from outside of the EU as to their declaration obligations.</li> <li>• One-year period of retention of most data in the INZOLL database considerably diminishes the utility of that database for analysis.</li> </ul>

### 3. PREVENTIVE MEASURES – FINANCIAL INSTITUTIONS

#### Law, regulation, and other enforceable means

548. As indicated above, the main relevant texts are the AML Act, which applies to all persons and entities subject to the AML/CFT framework, the Banking Act, the Investment Act and the Insurance Supervision Act. All four texts have been passed by the Federal Parliament, and they constitute primary legislation for the purposes of this assessment. The AML Act is accompanied by an extensive explanatory memorandum, which provides guidance on the background to, and intention of the provisions. While this memorandum helps clarify certain issues (and, under German constitutional law, is taken into account by the courts in their interpretation of the law), there are some circumstances in which it appears to interpret the provisions in a way that is different from the precise meaning of the actual text of the law (see, for example, the discussion of the STR obligation in Section 3.7). Since the AML Act has yet to be tested through the courts, there is no reason to believe that the language of the explanatory memorandum would have precedence over the language of the AML Act itself, or would have any direct force in law in its own right. Therefore, the memorandum is not regarded as other enforceable means (OEM) for the purposes of this assessment.

549. The BaFin has the powers to conduct AML/CFT supervision of the financial sector and to sanction noncompliance with AML/CFT measures in individual cases (Section 16 and 17(4) of the AML Act). In addition, it has powers to issue rules, regulations or other enforceable instruments, on the basis of the supervisory laws and the AML Act, with respect both to individual institutions and to single institutions or groups of institutions. Over the years, the BaFin has issued a number of circulars and letters (for the attention of all or part of the financial sector) that reflect its administrative practices. These lay out the BaFin's interpretation of the legal requirements and, as a consequence, they have a binding effect upon the BaFin in its dealings with the institutions, pursuant to the principle of equality of treatment, according to which public authorities must treat similar situations equally, based upon their interpretation of the law.

550. For the purposes of this assessment, the BaFin circulars and letters are considered as guidance only and do not constitute OEM. They are referenced, from time to time, where they are relevant to an understanding of the legal obligations. There are situations (see discussion of Recommendation 21) where the circulars provide specific information to institutions, which may be sanctioned under provisions of the primary legislation if they fail to take account of such information in the application of their risk-based approach. To this limited extent, specific circulars may have indirect enforceability, and such circumstances have been taken into account in this assessment.

551. Most of the BaFin circulars and letters are based on the previous law (the AML Act as amended in 2002). Many were withdrawn (through the BaFin Circular 2/2009 dated January 13, 2009) after the entry into force of the 2008 AML Act, largely because the key elements that they contained have now been incorporated into the primary legislation, or because some of the legal provisions which form the basis for the administrative practice have been changed significantly. However, the BaFin has advised institutions and the auditors that, where the contents of the repealed circulars do not conflict with the provisions of the new AML Act or with the initial guidance produced by the industry associations, it will continue to use the contents as the basis for its administrative practice, pending the publication of comprehensive new



guidance by the industry associations (see below). This procedure has caused some confusion in the financial sector about exactly which parts of the circulars remain valid.

552. The BaFin has indicated that, going forward, it is its intention to develop comprehensive guidance through the private sector associations. Under this arrangement, the industry associations will formulate the guidance, but it will receive official endorsement from the BaFin, and may, therefore, reasonably be relied upon by the financial services sector as reflecting the BaFin's understanding of the legal obligations. Any circulars or letters issued by the BaFin will simply support the industry guidance. While a comprehensive set of industry guidance is expected by end-2009 or early-2010, some interim documents were published previously, specifically:

- The Central Association of the German Banking Industry (*Zentraler Kreditausschuss, ZKA*) Guidelines in relation to the Act, issued on December 17, 2008;
- A similar document issued by the federal association of insurance companies (the *Gesamtverband der Deutschen Versicherungswirtschaft; GDV*) on February 18, 2009; and
- A similar document issued by the association of private building societies (*Verband der Privaten Bausparkassen*) and the federal coordination office of the state building societies (*Bundesgeschäftsstelle Landesbausparkassen*) issued in February 2009.

553. Other documents are also planned for a small number of specialist sectors, but the three foregoing guidelines are addressed to institutions that make up 90 percent of those covered by the AML Act. The current interim guidelines have targeted primarily those areas of the AML Act that were considered to be new and potentially challenging for the financial sector, especially the risk-based approach.

554. Due to the fact that the BaFin incorporated the contents of the industry guidelines into its administrative practice by giving them its official approval, the courts (in accordance with the principles of administrative law) have to take the guidelines into account when interpreting the law and the administrative practice of the BaFin. However, for the purposes of this assessment, there is no basis on which to consider these guidelines to be OEM, as defined by the FATF.

555. Some credit institutions reported that they find the current ZKA guidelines difficult to understand, partly because of the tabular and bullet-point format in which they have been presented, and that they lack sufficient specificity because they seek to address the needs of a very wide range of disparate institutions. In defense of this, the ZKA believes that the BaFin will take a fairly standard line with respect to compliance by all institutions subject to the AML Act, and that the guidelines provide a basis for understanding the BaFin's likely stance. There was a general sense that the guidelines were a useful development in that, for the first time, they would concentrate the BaFin's interpretations of the AML/CFT provisions into one place, rather than having a series of individual circulars over a period of years.

## Scope

556. The new AML Act applies to credit institutions, financial services institutions, financial enterprises,<sup>56</sup> insurance companies, insurance intermediaries and investment companies, as well as a broad range of nonfinancial sector persons or entities. The scope of the activities of all these entities is defined in the various regulatory laws, and covers the vast majority of the financial activities listed in the FATF

<sup>56</sup> Financial enterprises comprise a range of specialist service providers, include leasing companies, money brokers, and investment advisers. During the on-site assessment, Germany indicated that financial enterprises are regulated by the *Länder* authorities and not by BaFin. No further information was available.



glossary. The only exception to this is for pawnbrokers when they grant loans against pledges. Given that pawnbrokers only deal in small amounts of money, that their activity is limited to certain minor transactions and that they are, in any case, required under governing legislation to identify their customers by an ID card or passport, and to record the relevant information (including name, given name, birthday, place of residence, address, type, and issuing authority of the document presented to verify identity), the legislator deemed it unnecessary to include such operations in the definition of a credit institution or to subject them to the provisions of the AML Act. This appears to be a reasonable conclusion.

557. In the following description of the preventive measures, there is also reference to relevant provisions of the banking, insurance, and investment Acts. The scope of these Acts covers the majority of financial activities defined by the FATF. Exact details can be found in the main table in Section 1.3 of this report. Reliance on these laws for certain obligations not included within the AML Act does not constitute a material scope limitation.

### ***Customer Due Diligence and Record Keeping***

#### **3.1. Risk of money laundering or terrorist financing**

558. Section 2(2) of the AML Act provides that, through statutory instruments, the authorities may exempt persons from the Act where such persons engage in financial activity on an occasional or very limited basis, and where there is little risk of ML or TF. To date, there has been no specific exemption granted by the authorities, although foreign currency exchange by hotels, irrespective of the scale of that activity, is excluded from the definition of a financial services institution under the Banking Act (for “undertakings whose sole financial service is dealing in foreign notes and coins unless their main business is foreign currency dealing”).

#### **European “equivalence”**

559. Throughout this section of the report (Recommendations 5, 7, 9, 22, 23, SRVII) there are references to the applications of exemptions or certain specific “low-risk” measures, designated within the AML Act, with respect to institutions, transactions, counterparties, etc, that originate from or are based in other EU member states.<sup>57</sup> These designations are derived from the EU-wide regulations and directives, which work on the presumption that all member states have AML/CFT regimes of a minimum common standard, and can be treated, *de facto*, and sometimes *de jure*, by each member state as being part of its domestic environment. In certain very specific cases (*e.g.* SR. VII), the FATF has recognized within its standards, the validity of the single European framework. More generally, however, there is no presumption by the FATF that the treatment of all member states as being equivalent is appropriate in terms of a country fulfilling the requirements of the standards.

560. In addition, several of the preventive measures that have cross-border elements within the AML Act provide certain gateways, exemptions and “low risk” options with respect to third countries outside the EU, when they are deemed to apply the FATF standards on an equivalent basis to those applied within the EU. In implementing these provisions, the authorities instructed the financial institutions (through circular 7/2008) that they may rely on the EU member states’ “equivalence list,”<sup>58</sup> when determining which countries meet this test. This list, which has been established on a voluntary basis by member states,

<sup>57</sup> In some contexts, the equivalence presumption is extended to members of the European Economic Area, which includes Iceland, Norway, and Liechtenstein. In addition, the EC has a number of bilateral treaties with Switzerland which extend exemptions similar to the EEA exemptions.

<sup>58</sup> Derived from the “Common Understanding on the Criteria for the Recognition of Third Countries Equivalence under the Third Anti-Money Laundering Directive.”

comprises all non-EU member jurisdictions of the FATF (and also includes the French and Dutch overseas territories, on the basis that they are deemed to be part of the metropolitan countries' membership of the FATF). No independent risk assessment of the countries on the list has been undertaken by the German authorities outside the assessment by representatives of the EU-member states, including participants from the BMF and the BaFin. However, it was observed during the assessment that the institutions themselves found the blanket approach to "equivalence" to be counter-intuitive, and most reported that, notwithstanding the official list, they undertake their own risk assessment for all countries, including members of the EU.

561. In July 2009 (subsequent to the assessment mission), the BaFin issued a circular seeking to clarify its position on the use of the equivalence list. The circular specifies that "an institution or a financial sector undertaking from a country mentioned therein applies due diligence requirements that are equivalent to the requirements within the European Union. The third-country equivalence list does not, however, mean that institutions or financial sector undertakings that have their registered office in the countries or areas listed therein can always be routinely assumed, despite any indicators in any particular case of an enhanced risk situation, to present a low risk." The circular goes on to state that institutions would be expected to undertake appropriate due diligence if they had reason to believe that the customer, transaction, etc. does not represent a low risk. In addition, the circular extends these principles to "business relationships or transactions with institutions or financial sector undertakings that are based in other EU Member States." Institutions are specifically referred to the FATF's mutual evaluations as a source of material to assist their risk analysis.

562. The July 2009 circular is helpful guidance, but it does not entirely remove the specific concerns raised elsewhere in this report. Consequently, where relevant in this report, the assessors have taken the view that the generic categorization of all EU member states, EEA states and other FATF member jurisdictions as adequately applying the FATF standards is unreasonable, in the absence of a proper risk assessment by the authorities that takes into account the specific risks for the German environment. In this context it has also to be noted that four member states of the EU have still failed to implement the provisions of the Third EC Money Laundering Directive, which provides the basis for member states' comparability, and the assessment reports of other FATF member jurisdictions show significant variations in the application of the standards.

## **3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)**

### **3.2.1 Description and Analysis**

#### ***Legal Framework***

563. The German customer due diligence (CDD) and record-keeping requirements are set out in the AML Act. The Act came into force on August 21, 2008 pursuant to Article 2 of the Act to Enhance the Fight against Money Laundering and Financing of Terrorism and replaced the 2002 AML Act. It is part of the legislative package that was adopted by Germany to implement the Third EC Money Laundering Directive (Directive 2005/60/EC) and the implementing Directive (Commission Directive 2006/70/EC) into its national legislation. This legislative package also entailed amendments to the Banking Act, the Insurance Supervision Act, the Investment Act, the CC (more specifically the ML offense) and the CAA.

564. It is important to note that this assessment does not address the effective transposition of the Third EC Money Laundering Directive into national law by Germany, but rather the level of compliance by Germany with the FATF standards. Therefore, although there may be circumstances where the German legislation and practice are entirely compatible with the Directive, the assessors have noted where, in their view, the provisions do not comply with the FATF standards.

565. All financial institutions that carry out activities captured by the AML Act are supervised by the BaFin for AML/CFT purposes, except: the KfW<sup>59</sup> (which is subject to MoF supervision but not for AML/CFT purposes); three insurance companies that are active within single *Länder* (and are subject to the *Land* insurance supervisors); brokering of closed-end real estate funds; pawnbrokers; and insurance intermediaries.

566. The AML Act strengthened the CDD and record keeping requirements that were already in place in Germany and, for the first time, explicitly introduced a risk-based approach to the implementation of CDD measures. The AML/CFT preventive measures apply equally to all persons and entities subject to the Act. Additional CDD provisions have, however, also been laid out in the amendments to the sector-specific laws, in particular the Banking Act, the Investment Act and the Insurance Supervision Act, in order to address issues relevant only to those sectors.

### ***Prohibition of Anonymous Accounts (c. 5.1)***

567. The current legal framework sets out identification requirements in a way that prohibits the establishment of anonymous accounts and accounts in fictitious names. Section 154 of the Fiscal Code, which has been in force since 1932, provides that “no one may under a false or fictitious name, for [oneself] or for a third person, open an account or cause entries to be made in an account, give into safe custody or pledge valuables (money, securities, precious objects) or rent a safety deposit box”. It also imposes an obligation on those (*i.e.* in practice only credit institutions) who keep accounts, hold valuables in safe custody or as a pledge, or rent out a safety deposit box “to make certain before doing so of the identity and the address of the authorized drawer” and to “record the relevant particulars in suitable form.” According to the authorities, the term “account” is interpreted broadly and covers, for example, sub-accounts as well as trust accounts held by notaries or lawyers. Numbered accounts are not a feature of the German banking system.

568. The 2008 AML Act requires the identification of the contracting parties and the beneficial owners. It defines “identification” as covering both the establishment of the identity by gathering information and the verification of the identity, although the basis upon which verification has to be undertaken is subject to subsequent refinement in the Act (see discussion below of beneficial ownership). Given the longevity of the Fiscal Code (subsequently reinforced by successive AML Acts), there is no reason to believe that anonymous accounts are prevalent in Germany.

### ***When is CDD required (c. 5.2)***

569. The AML Act clearly defines the circumstances in which customer identification is required. Under Section 3(1) and 4(1), all persons and institutions covered by the AML Act are required to identify the contracting parties and beneficial owners in the following circumstances laid down in Section 3(2):

- **When establishing a business relationship**, defined in the Act as “a business or professional relationship which is directly connected with the professional activities of the institutions and persons covered by [the] Act and which is expected, at the time when the contract is established, to have an element of duration.”

<sup>59</sup> The KfW has a specific public function, *i.e.*, the provisions of development loans in the public interest. Its customer base consists of German towns and other public entities at the *Länder* level and its capital is provided by the Federal and *Länder* governments. However, it has a subsidiary banking entity that is subject to AML/CFT supervision by the BaFin.

- **When carrying out occasional transactions amounting to EUR 15 000 (USD 20 876) or more**, whether the transaction is carried out in a single operation or in several operations totaling EUR 15 000 (USD 20 876) or more which appear to be linked. For the purposes of the AML Act, “transaction” has been defined as “any act aimed at or resulting in a transfer of money or a similar movement of assets.” Exceptions to this general rule have been made for exchange companies and money remitters under Section 25f(3) of the Banking Act, in situations where the transaction is taking place other than from an existing account held by the customer. In the case of the exchange companies the threshold for CDD is reduced to EUR 2 500 (USD 3 479) in such circumstances, and to zero in the case of money remitters. In addition, full identification must be undertaken for each and every transaction, even if the remitter or exchange company has already dealt with the customer before, and has a record of his or her identity.
- **When there is reason to suspect money laundering or terrorist financing**, regardless of any derogation, exemption or threshold.
- **When there are doubts about the veracity or adequacy of data** identifying the contracting party or the beneficial owner. However, this provision is partly weakened by the provisions relating to low-risk customers (see below).

570. In addition, under Article 5(2) of the EU Regulation 1781/2006 which implements directly throughout the European Union the provisions governing wire transfers (see discussion of SRVII), a payment services provider, before transferring funds, has to identify all customers, and verify identity wherever the transfer is for a value of EUR 1 000 (USD 1 392) or more.

571. It is important to note that the AML Act also explicitly waives the broader customer due diligence requirements in a large number of “low-risk” circumstances specified under both the AML Act and the Acts relating to the banking and insurance sectors. These (and the potential difficulties arising from them) are described in more detail below when discussing the simplified due diligence arrangements.

***Identification measures and verification sources (c. 5.3); Identification of Legal Persons or Other Arrangements (c. 5.4)***

572. The AML Act provides specific instructions as to the basis for identification and verification of the customer. Pursuant to Section 4(3), in order to establish the identity of the contracting party, the following information must be gathered:

- For **natural persons**: name, place and date of birth, nationality and address. According to the explanatory memorandum to the AML Act, the “name” is actually the full name, *i.e.* the surname and at least one given name.
- For **legal persons or partnerships**: company name or title, legal form, registry number if available, address of headquarters or head office, names of members of the representative body or legal representatives. If a member of the representative body or legal representative is also a legal person, its name, legal form, registry number and address must also be obtained.

573. Section 4(4) requires the verification of identity on the basis of the following documents:

- For **natural persons**: a valid official identity card including the holder’s photograph, which satisfies domestic requirements for identity cards or passports, in particular domestic passports, identity card or their substitutes recognized or accepted under foreign laws. The explanatory

memorandum to the Act provides extensive further information on the type of documents which are suitable for identification and verification purposes for both German and foreign nationals, although the basic presumption is that the documents must have the same status as either an identity card or passport issued by the German government. There are limited exceptions to this rule in cases where the potential customer does not have identification documents, specifically when the contracting parties are minors or are subject to custodianship. Identity documents are required for all German citizens over the age of sixteen (Section 1 of the Passport Act), and for all foreigners with residency permits.

- For **legal persons or partnerships** (to verify the legal identity only of the customer): a copy of the relevant entry in the commercial register or register of cooperative societies or similar official register; foundation documents or equivalent documents.

574. While there is no reference in this provision to the measures required with respect to legal arrangements (trusts or *Treuhand*), Section 1(6) of the AML Act includes such arrangements within the scope of the definition of beneficial ownership, for which identification measures are required. However, this provision defines the beneficial owner as the natural person(s) who exercises control over 25% or more of the property of a legal arrangement, **or who is** the beneficiary of 25% or more of such property. While this definition would cover the trustee and beneficiaries of a trust (and similar relationships with respect to a *Treuhand*), it does not address the identity of the settlor (who legally relinquishes control on settlement of the trust, but who is captured under the FATF definition of beneficial owner) or any other parties that might be involved in the arrangement. This is a significant gap in the coverage, given that the provision of financial services to legal arrangements appears to be relatively common in Germany.

#### ***Identification of Beneficial Owners (c. 5.5; 5.5.1 & 5.5.2)***

575. There is a general requirement (Section 3(1) number 3 of the AML Act) for all institutions and persons to “clarify whether the contracting party is acting on behalf of a beneficial owner and, if so, to identify the beneficial owner,” although this is not applicable in respect of the specified low risk scenarios (see below). The requirement to identify the beneficial owner as well as the contracting party is repeated under Section 4(1) of the Act. Section 1(6) defines “beneficial owner” as “the natural person(s) who ultimately owns or controls the contracting party, or the natural person on whose behalf a transaction or activity is being conducted. This includes, in particular:

- In the case of **corporate entities which are not listed** on a regulated market as defined in Section 2 (5) of the Securities Trading Act and are not subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards: the natural person(s) who directly or indirectly hold more than 25% of the capital shares or control more than 25 percent of the voting rights;
- In the case of **legal entities**, such as foundations, and **legal arrangements**, such as trusts, which administer and distribute funds or arrange for third parties to administer and distribute funds:
  - a. The natural person(s) who exercises control over 25% or more of the property of a legal arrangement or entity;
  - b. The natural person(s) who is the beneficiary of 25% or more of the property of a legal arrangement or entity;
  - c. Where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates.



576. The explanatory memorandum to the AML Act provides that the cases referred to above are only examples. It also provides that some type of legal persons present a higher risk of being misused for ML or TF purposes, taking the example of the civil-law partnerships,<sup>60</sup> which may lack transparency because they may not be registered. In these cases, the institutions and persons covered by the Act “should be guided not only by the threshold of 25% participation” but “when conducting due diligence, should rather pay special attention to assessing the specific risk inherent in the business relationship or transaction with the civil-law partnership and decide the risk-sensitive fashion which partner should be identified as the beneficial owner.” The ZKA guidelines provide extensive further guidance on appropriate procedures to identify beneficial ownership in multi-layer corporate structures.

577. With respect to customers that are legal persons or arrangements, Section 3(1) number 3 of the AML Act specifically provides that the requirement to identify the beneficial owner includes the duty to take adequate measures to understand the ownership and control structure of the client. However, this requirement is not applicable in respect of the specified low risk scenarios (see below).

578. Section 4(5) specifies that institutions “shall find out at least the name of the beneficial owner and gather further identification depending on the level of risk of money laundering or terrorist financing in the individual case.” The explanatory memorandum elaborates on this by stating that “further identifying features such as address, date of birth and nationality need only be gathered where appropriate” given the ML/TF risks. This clearly sets a lower standard than is required of the contracting party itself, where the law specifies that certain minimum information must be obtained in all cases. As regards verification of identity, Section 4(5) requires that institutions “take risk-adequate measures to check the accuracy of the information gathered.” This suggests that in situations presenting a “normal” level of risk, it might be sufficient simply to establish the name of the beneficial owner; and only in situations presenting a higher risk would the full establishment and verification of the beneficial owner’s identity be made necessary. This falls short of the FATF standards, which require that in all cases (unless there are specific low-risk situations) institutions should take reasonable measures to verify the identity of customers. Subsequent to the on-site visit, the BaFin issued a circular (Circular 14/2009 of July 30, 2009) which explicitly affirms its view that the term “take risk-adequate measures” requires that some measures to verify the identity of the beneficial owner must be taken in all cases. The circular also counters the statement in the ZKA guidance that reliance for verification may be placed on information provided by the contracting party.

579. This clarification of the BaFin’s interpretation is important, since, from discussions with the financial institutions and professional associations, it was apparent that there was a variety of practices and understandings of the obligation. In some cases, the perception was that, if the customer is a corporate entity, the shares of which are held by other corporate entities, the obligation extends only to verifying the identity of the first tier of shareholders, and not to “drill down” to the underlying natural persons. In other cases, the view was that, indeed, the ultimate natural persons should be traced back, but only through the channels where the immediate registered shareholding of the customer breached the 25% threshold. This might mean that the link between related parties at a higher level of the ownership chain might not be recognized. In yet other cases, the view was taken that there would be no basic presumption that the beneficial ownership was required to be verified unless the situation was assessed to be high risk. In all cases, there seemed to be a degree of uncertainty about what the verification process actually required in such circumstances. This wide variety of interpretations did not appear to arise simply from different applications of the risk-based approach, but rather from uncertainty as to exactly what is required. The result is that there could be no comfort, at the time of the mission, as to the level of implementation of procedures to verify the identity of the ultimate natural persons who own or control the customer.

<sup>60</sup>

A civil law partnership (*Gesellschaft bürgerlichen Rechts, GbR*) is defined as an association of individuals or enterprises united in the achievement of a joint contractual purpose. It is suitable, for example, for both start-ups launching a business idea in cooperation with others and for a lottery syndicate.



***Information on Purpose and Nature of Business Relationship (c. 5.6)***

580. Under Section 3(1) number 2 of the Act, institutions are required to seek and obtain information on the purpose and the intended nature of the business relationship, “if the business relationship does not already make them clear beyond doubt.” The requirement does not apply to defined “low-risk” situations. The ZKA guidelines elaborate on this by indicating that certain products (*e.g.* giro accounts for general payments or a securities account) would normally be self-evident with respect to their purpose and would not require further enquiries. These include the bulk of products sold at the retail level to natural persons.

***Ongoing Due Diligence on Business Relationship (c. 5.7; 5.7.1 & 5.7.2)***

581. The AML Act (Section 3(1) number 4) explicitly requires all institutions to monitor continuously the business relationship, except with respect to the specified low-risk situations. This monitoring includes “scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution’s or the person’s knowledge of the contracting party and beneficial owner, if applicable, the business risk profile, including, where necessary, the source of funds, and ensure that the documents, data or information are updated at appropriate intervals”.

582. Additional provisions have been incorporated into the sector-specific regulatory laws, as follows:

- **Credit institutions:** Section 25 c (2) of the Banking Act requires the implementation of an appropriate data processing system to support the monitoring function. It provides that credit institutions must — as part of their proper business organization and appropriate risk management to prevent fraudulent activities — create and update internal policies and adequate business and customer-related safeguards, and conduct checks. They must also operate and update appropriate IT systems, which enable them to identify business relationships and individual transactions in payment operations that appear dubious or unusual. Where such circumstances are identified, they must be investigated in the context of the current business relationship and individual transactions in order to be able to monitor and assess the risk involved in the relevant business relationships and transactions and, if necessary, examine whether there are grounds for suspicion. The BaFin can define criteria for cases in which credit institutions are not required to use data processing systems and has made use of this possibility for smaller cooperative banks.
- **Insurance companies:** Section 80d(1) of the Insurance Supervision Act repeats the monitoring obligation set out in the AML Act. It also allows insurance companies to use data processing systems, although, unlike for the credit institutions, these are not mandatory.

583. The exemptions provided with respect to low-risk situations give rise to some uncertainty about what obligations actually exist in respect of the ongoing monitoring of such relationships (see detailed discussion below).

***Risk – Enhanced Due Diligence for Higher Risk Customers (c. 5.8):***

584. Section 6(1) requires that institutions must apply enhanced due diligence measures in situations that are assessed, through their own risk analysis, to be higher than normal risk. In addition, Section 6(2) lists two specific circumstances where enhanced due diligence must always be applied, and describes the type of additional measures required. These relate to politically-exposed persons (PEPs) and non-face-to-face relationships (see detail under Recommendations 6 and 7 below). Provision is also made for the

authorities to specify additional cases of high-risk situations, but only on the basis of a decision of the European Commission. No such designations have yet been made.

585. However, the overall provision is not intended to be limited to such specific circumstances, and there is a broader obligation in Section 3 of the Act for institutions to be able to demonstrate to the authorities that they have applied appropriate measures to the risks identified within their business. The explanatory memorandum makes it clear that the high-risk situations specified in the law are not exhaustive, and provides an example of country risk as another aspect to be noted by institutions. The ZKA guidelines provide additional insight into what approach institutions might take in identifying and addressing high-risk situations, but the extent of overall guidance is somewhat limited.

***Risk — Application of Simplified/Reduced CDD measures when appropriate (c. 5.9); Simplification/Reduction of CDD measures relating to overseas residents (c. 5.10); Simplified/Reduced CDD measures not to apply when suspicions of ML/TF or other high risk scenarios exist (c. 5.11); Risk Based Application of CDD to be consistent with Guidelines (c. 5.12)***

586. The AML Act, the Banking Act, the Investment Act, and the Insurance Supervision Act provide for exceptions to the standard CDD requirements, and, in so doing, give rise to broader problems. Section 5(1) of the AML Act provides that, in certain specified circumstances (and unless the institution assesses that there is a higher risk of ML or TF or suspects that a transaction is linked to such activities), an institution is exempted from the provisions of Section 3(1) of the Act, which addresses the key CDD components of verifying the customer's identity, identifying the beneficial owner, obtaining information on the purpose and intended nature of the business relationship, and conducting ongoing monitoring of the relationship. This exemption applies with respect to customers who are:

- German credit institutions, financial services institutions, financial enterprises, insurance companies, and insurance intermediaries, as well as credit or financial institutions from another EU member state or a third country that applies equivalent requirements and supervision to those applied in Germany.
- Listed companies whose securities are admitted to trading on the German market or in one or more EU Member state, as well as listed companies from a third country that are subject to disclosure requirements consistent with EU legislation.
- Domestic public authorities (both from the federal and *Länder* levels), as well as other EU member state public authorities or institutions provided that their identity is publicly available.

587. The exemption also applies to the identification of the beneficial owner of third-party accounts of lawyers, when the information on the identity of the beneficial owner is available upon request, as well as similar accounts held for notaries and other independent legal professionals from an EU member country or a third country that applies AML/CFT measures and supervision consistent with the international standard.

588. In addition to the exemptions listed above, the Banking Act and the Investment Act (Section 25d) and the Supervision of the Insurance Industry Act (80e) extend the same exemption to a lengthy list of specific transactions that are subject to a variety of limits in terms of amount, type of counterparty, residence of counterparty and type of business (for the details of these exemptions, see relevant amendments to these provisions embedded in the AML Act in the annex to this report).

589. The explanatory memorandum and the industry guidelines indicate that the statutory lists are definitive, and that institutions cannot avail themselves of the concessions through their own analysis of

other low-risk customers and transactions. However, there is some confusion in the various texts supporting the Act as to whether the exemptions are mandatory in the circumstances defined, or whether an institution's own assessment of the customer being a higher risk can override the legal categorization. The Act itself (supported by the explanatory memorandum) clearly indicates that institutions should apply an override in the event that they consider specific situations not to be low risk, but the ZKA guidelines state that "the system introduced by the new law distinguishes between special statutory rules applicable to certain groups or categories of cases...subject to generalized, predetermined risk classifications, requiring either increased or simplified due diligence obligations; and those provisions leaving room for discretion for individual solutions by institutions. Room for discretion exists with regard to all aspects of the customer due diligence obligations, provided there are no specific statutory requirements concerning high **or low** risks" (emphasis added). On the basis that the primary Act is unambiguous, it has to be assumed that institutions will treat the measures as discretionary within the context of their overall risk analysis, but the guidelines would benefit from clarification.

590. In general, the exemptions give rise to a number of concerns about the impact on the integrity of some of the CDD measures. The list of exemptions has been taken directly from the Third EC Money Laundering Directive, which only mandates simplified procedures in respect of customers who are credit or financial institutions within the EU, or in third countries that impose requirements equivalent to those of the Directive. In all other cases, the specified concessions are at national discretion, but, as explained in Section 3.1 above, the German authorities have not undertaken any formal risk analysis to determine whether the circumstances are appropriate to the local environment.

591. While the FATF standard allows for the application of CDD measures on a risk-sensitive basis, it specifies that in low-risk situations institutions, may apply "reduced or simplified measures." From this, it has to be assumed that some degree of due diligence must be undertaken in all cases, and that the standards do not allow for a complete exemption in the case of individual customers or transactions. In the circumstances provided under the AML Act, it is apparent that, in the defined set of "low-risk" circumstances, institutions are specifically exempted from the vast majority of the key elements of the CDD process, although the process of basic identification appears to be assured under Section 4(1) which repeats the need to identify the contracting party and beneficial owner outside the context of the exempted provisions in the Act.

592. Even were the list of exempted customers and transactions to be appropriate on a risk-sensitive basis with respect to initial due diligence procedures, there are two other areas of particular concern. The first is the removal of the obligation for institutions to undertake ongoing monitoring of the accounts to ensure that the transactions are consistent with the institution's knowledge of the customer, and therefore, to be in a position to identify suspicious transactions. The explanatory memorandum and the ZKA guidelines seek to reintroduce the concept that such an obligation does, in fact remain, but this is at odds with the text of the AML Act. Moreover, even if the obligation to monitor for unusual or suspicious transactions is not adversely affected by the exemption (and it is difficult to see how it is not), the institution would appear to be under no obligation to ensure that documents, data and other information are maintained on an accurate and up-to-date basis for such customers.

593. The second area of particular concern is the fact that the exemption applies even in cases where there are doubts about the veracity or adequacy of the information identifying the customer or beneficial owner. It might be argued that there is some logic in this exemption since an institution would not have reliable information in the first instance, but the overall tone of the provision runs counter to the concept that institutions should have core accurate information on their customers, whatever the risk. The "low-risk" exemption is not applicable in the event that the institution has reason to suspect that the transaction is related to ML or TF.

594. The authorities have indicated that they are aware of the unintended consequence of the strict implementation of the Third Directive, and that, as a consequence, they have been stressing upon institutions the need to have an effective monitoring system for suspicious transactions, regardless of any strict interpretation of the law. This message is contained in both the explanatory memorandum to the AML Act and the ZKA guidelines.

595. In practice, the exemptions provided with respect to the multitude of low-risk scenarios listed in the banking, investment and insurance legislation (as opposed to those in the AML Act) appear to have little practical application as far as the institutions are concerned, and therefore may not create any particular gaps in the system. All the institutions to which the assessment team spoke indicated that the complexity of the circumstances in which the exemptions apply is such that it would be very costly (and with minimal benefit) to factor the conditions into their control and monitoring systems. As a result they do not take account of the exemptions, and treat all such cases as standard risk.

#### ***Timing of Verification of Identity – General Rule (c. 5.13)***

596. Section 1(1) of the AML Act indicates that the term “identification” means both identification and verification. Section 4(1) provides for the basic rule that institutions should identify the contracting party and the beneficial owner before establishing a business relationship or carrying out a transaction. However, it goes on to state that identification may be completed while the business relationship is being established “if this is necessary to avoid interrupting the normal conduct of business and where there is little risk of ML or TF occurring”.

#### ***Timing of Verification of Identity – Treatment of Exceptional Circumstances (c.5.14 & 5.14.1)***

597. Exceptions to the general rule on timing are provided in the banking, investment and insurance legislation. Section 25e of the Banking Act and an equivalent provision in the Investment Act provides that credit and financial institutions may complete the verification of the identity of the contracting party and the beneficial owner “promptly after an account or deposit is opened.” To mitigate the risk this may cause, it also requires credit institutions to ensure that no funds can be withdrawn from the account before the verification of identity has been completed. In the event that the identity cannot subsequently be verified, the BaFin would expect institutions to return the funds directly to the source from where they came, but this is not referenced in the legislation. However, under the Civil Code, Section 812 ff, the provisions on “unjustified enrichment” (*ungerechtfertigte Bereicherung*) may prevent the funds from being diverted to a third party.

598. Section 80f(3) of the Insurance Supervision Act provides for a general principle that verification of the identity of the designated beneficiary of an insurance policy may be undertaken after the business relationship has been established, provided that verification is completed before any benefits are paid out or before the beneficiary intends to claim any rights under the policy.

#### ***Failure to Complete CDD before commencing the Business Relationship (c. 5.15) & Failure to Complete CDD after commencing the Business Relationship (c. 5.16)***

599. Under Section 3(6) of the AML Act (and in circumstance other than those that have been subject to exemption), if a person or entity covered by the Act is unable to fulfill the CDD requirements, it may not establish or continue a business relationship or carry out any transactions, regardless of any legal or contractual provisions. There is, however, no requirement to consider filing an STR in case of failure to complete CDD.

600. According to the authorities, notwithstanding the terms of Section 3(6), the obligation to terminate the business relationship in case of failure to complete the CDD is subject to the fundamental

legal principle of proportionality and to the risk-based approach. This is also in the context of the general presumption that everyone in Germany has the right of access to financial services. Under Section 4(6), the obligation is placed on the customer to provide all necessary information and documentation (rather than upon the institution to acquire it), and so the institutions will be in a position to refuse or close an account on the grounds that the customer has failed to meet his or her legal obligation.

***Existing Customers – CDD Requirements (c. 5.17)***

601. There is no explicit requirement in the law to conduct CDD on existing clients, but, instead, reliance is placed on the provisions of Section 3(1), number 4, which requires institutions to “ensure that documents, data or information are updated at appropriate intervals.” The explanatory memorandum clarifies that this provision is intended to be read in the context of a requirement to apply measures to existing customers at appropriate times. From discussions with the authorities and relevant institutions, it is apparent that such procedures are risk-based, and that the interlude between substantive reviews of individual customers will be determined either by the risk category to which individuals have been assigned, or by the occurrence of an unusual event or transaction. The authorities have indicated to the institutions that, in the case of customers that do not pose a high risk, a timeframe of two to ten years for a complete review of a customers’ file would not be unreasonable. Given the substantive new elements for the CDD process introduced by the new AML Act, the outside time limit appears excessive even for the lowest-risk category; but, from discussions with the institutions, it appears that they seek to apply much shorter timeframes for their reviews. It would be preferable for the authorities to bring their requirements more into line with the market practice. It is also unclear what is expected of institutions in respect of their “statutory” low-risk customers, since they are exempted from the provisions of Section 3(1) in such cases, although both the explanatory memorandum and the industry guidelines suggest that some degree of ongoing monitoring is required in such cases.

***Existing Anonymous-account Customers – CDD Requirements (c. 5.18)***

602. There is no history of anonymous accounts in Germany due to the long-standing provisions of the Fiscal Code, and so no measures are required in respect of identifying such account holders.

***Foreign PEPs – Requirement to Identify (c. 6.1); Risk Management (c. 6.2; 6.2.1); Requirement to Determine Source of Wealth and Funds (c. 6.3); Ongoing Monitoring (c. 6.4)***

603. Section 6(2) of the AML Act requires institutions to take risk-based measures to determine whether the contracting party is a PEP. Where this is determined to be the case, institutions are obliged, prior to commencing the relationship:

- To require staff to seek approval from an “immediate supervisor or next higher management level” before establishing the relationship;
- To apply appropriate measures to determine the origin of the assets to be used in the business relationship; and, thereafter,
- To subject the relationship to continuous enhanced oversight.

604. There is no obligation in the Act addressing the situation where an existing customer becomes, or is subsequently found to be a PEP, although there may be a presumption that this should form part of the institutions’ normal risk management procedures (and the BaFin has subsequently issued guidance to this effect in its circular of July 2009). In addition, the specified approval procedures require referral simply to the immediate supervisor or to next level of management, without there being any certainty that this would



constitute “senior management,” as required by the FATF standard. The FATF does not define what it means by “senior management,” but there must be a presumption that it should preclude the possibility of approval being given by a junior or middle-ranking supervisor or manager, which appears to be permissible under the terms of the AML Act.

605. However, a more fundamental issue arises with respect to the underlying definition of who constitutes a PEP. Section 6(2) of the AML Act defines a PEP by direct reference to the Implementing Directive for Third EC Money Laundering Directive, to include “natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates of such persons.” Since the obligation on the institution is to establish the status of the contracting party, there is no specific requirement to establish whether the beneficial owner of the contracting party might be a PEP. Section 6(2) does make reference to the need to clarify whether the contracting party is a close associate of a PEP, but limits this to circumstances where the fact of the association is known to the public or where the institution has reason to believe this to be the case. Enhanced due diligence is required where a close associate is identified as being the sole proprietor of a legal entity or arrangement that is known have been set up for the benefit of the PEP.

606. Furthermore, Section 6(1) limits the scope of the PEP requirement to individuals who are “based outside the country,” and who have not been in a politically-exposed position for one year or more. In practice, these provisions would mean that a person who holds a relevant position, but who resides in Germany, is not covered; nor would it cover someone who, wherever their residence, might retain the proceeds of stolen state assets a year after leaving office. In practice, it might be assumed that an institution would categorize such circumstances within their high-risk group of customers (and the BaFin has subsequently issued guidance to this effect in its circular of July 2009), but the specific provisions of Section 6(2) would not apply. More generally, the FATF plenary has considered the one-year limit in the context of another EU member state’s mutual evaluation report, and has concluded that such a threshold is not a material deficiency when there is a general obligation to apply enhanced due diligence to customers (including PEPs) who still present a higher risk of ML or TF regardless of any timeframe. Section 6(1) of the German AML Act provides for such an obligation.

#### ***Domestic PEPs – Requirements (Additional Element c. 6.5)***

607. The requirements described above have not been applied to domestic PEPs.

#### ***Domestic PEPs – Ratification of the Merida Convention (Additional Element c. 6.6)***

608. Germany has signed, but not yet ratified, the Merida Convention.

#### ***Cross-Border Correspondent Accounts and Similar Relationships – introduction***

609. According to Section 25f(1) of the Banking Act, credit institutions must apply enhanced due diligence measures in their business relationships with respondent institutions based in “third countries.” Although this term is not defined in the Act, the authorities have indicated that the obligation under Section 25f(1) relates to respondent institutions in non-EU countries only. There are no specific provisions that address intra-EU relationships, which are deemed generically to be low risk under Section 5(2) of the Act. The requirement under Section 25f(1) is specified to be in addition to the enhanced due diligence obligations under Section 6 of the AML Act. However, while Section 6 makes reference to enhanced procedures, in general, it only specifies what constitutes such procedures in the cases of PEPs and non-face-to-face relationships. By reference to Section 3(4) of the AML Act, the provision suggests that institutions may determine the extent of due diligence measures on a risk-sensitive basis, since an institution must be able to demonstrate to the BaFin that the extent of the measures it has taken are



commensurate to the risk. The authorities have indicated that this is intended to provide some flexibility for institutions to be able to differentiate, for example, between FATF countries and other non-EU countries. However, given the very specific obligations under Section 25f(2), as described below, further clarification is required about what measures institutions are expected to adopt under the first, more general, subsection, but this, in itself, does not adversely affect the overall intention of this section of the Act.

***Requirement to Obtain Information on Respondent Institution (c. 7.1); Assessment of AML/CFT Controls in Respondent Institution (c. 7.2); Approval of Establishing Correspondent Relationships (c. 7.3); Documentation of AML/CFT Responsibilities for Each Institution (c. 7.4); Payable-Through Accounts (c. 7.5)***

610. Section 25f(2) specifies the procedures that institutions must adopt when engaging with a non-EU-based bank. It requires that credit institutions:

- a. Both before establishing a correspondent business relationship and during such a relationship, gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and management structure; to determine from publicly available information the reputation of the institution and the quality of supervision; and to assess the respondent institution's controls to prevent ML and TF;
- b. Before establishing such relationships, define and document the respective responsibilities of each institution with respect to meeting due diligence requirements;
- c. Before establishing such a relationship, obtain approval from a superior or next level of management;
- d. Take measures to ensure that the respondent institution does not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank; and
- e. Take measures to ensure that respondent institutions do not allow transactions via payable-through accounts.

611. The last measure on payable-through accounts appears to apply an obligation on the institution to establish whether its respondent institution is offering payable-through accounts anywhere, irrespective of whether this applies to the facility that the institution itself is providing to the respondent. If so, this is a relatively high hurdle, but the general intent is reinforced by Section 25f of the Banking Act, which expressly prohibits the establishing or managing of accounts in the name of the credit institution or a third-party institution, where the accounts may be accessed independently by customers to carry out their own transactions.

612. The explanatory memorandum to Section 25f(2) largely repeats the concepts contained in the statutory provision, but does indicate that no correspondent banking relationships should be established with institutions located in third countries that are not subject to effective supervision, especially with regard to ML. At the same time it indicates that, for existing relationships, enhanced due diligence is expected when the respondent bank is located in a country or region that is not a FATF member or does not comply with international AML/CFT standards.

613. In addition, before Section 25f of the Banking Act was introduced, the BaFin's predecessor organization issued a Circular, dated November 6, 2000, to all credit institutions, which included certain requirements for correspondent banking relationships. This circular is deemed still in force by the BaFin within the context of the new legislation, and specifies certain cautionary measures with respect to both the

institutional relationship (especially involving banks from countries outside the EU, FATF or Basel Committee membership) and the transactions being channeled through the correspondent account.

614. Generally, there appears to have been a high awareness of the risks associated with correspondent banking relationship over an extended period of time, and there is no indication that institutions are not applying appropriate measures within the confines of the Banking Act. However, although the AML Act requires the adoption, generally, of a risk-based approach, the Banking Act prescribes the specific measures only in the context of non-EU respondent banks, on the basis that respondent institutions headquartered in the EU are low risk, as specified in the Third EC Money Laundering Directive. This approach falls significantly short of the FATF standard, since the FATF has identified that correspondent banking *per se* is a high-risk activity that requires enhanced due diligence measures in all cases. It does not provide for the application of a risk-based approach in this area, and so the question of whether EU equivalence is appropriate is irrelevant in the context of Recommendation 7. The German authorities have stated that the nonapplicability of the requirements to EU correspondent relationships is in line with the FATF's recognition of the EU as a single jurisdiction, whereas Recommendation 7 addresses cross-border relationships. However, this argument has not been accepted by the assessors on the grounds that the FATF has made specific provisions for intra-EU transactions only in relation to Special Recommendations VII and IX. There is no recognition that intra-EU correspondent relationships should be treated as if they were domestic structures, thereby taking them outside the scope of Recommendation 7

***Misuse of New Technology for ML/TF (c. 8.1)***

615. There are no specific obligations with respect to mitigating the risks associated with technological developments. Instead, reliance is placed on Section 9(1) of the Money Laundering Act, under which financial institutions are obliged to take adequate internal measures to ensure that they cannot be misused for the purpose of ML and TF. Under circular 8/2005, financial institutions are advised by the BaFin to create their own analysis of potential risks across the board, taking into account, *inter alia*, the risks stemming from their businesses, the services offered and the means of their delivery. The BaFin has indicated that the risks created by the use of new technologies are expected to feed into the institution's risk analysis, if they are relevant.

616. The authorities have, on occasions, provided guidance to the institutions on the risks generated by new technologies. For example, the BaFin translated into German the FATF's 2006 typology report on New Payment Methods, and forwarded it to all financial institutions under its supervision (under cover of Circular 7/2008), and posted the document on its website. In addition, under an arrangement between the BaFin and the FIU, institutions have been provided with the password to access the FIU's Newsletter, which reports on the latest trends and techniques in crime, including specific AML/CFT typologies.

***Risk of Non-Face to Face Business Relationships (c. 8.2 & 8.2.1)***

617. Prior to the introduction of the new AML Act in August 2008, there was no specific provision permitting the establishment of a new business relationship without identification and verification of the customer by means of actual documents, such as a passport or ID card. Even where the customer is identified using a qualified digital signature according to Section 2(3) of the Digital Signature Act, such a signature is only granted if the applicant has been identified and verified by means of a passport or ID card (Section 5(1) Digital Signature Act in conjunction with Section 3(1) of the Digital Signature Ordinance). Moreover, the BaFin's 1998 Guidelines on AML/CFT measures established a general principle that customers should be identified in person either by the institution itself or by an authorized third party.

618. Specific non-face-to-face identification procedures have only been permitted since the new AML Act came into force. Section 6(2) of the Act explicitly mentions the possibility of non-face-to-face identification, and defines it as a case where enhanced due diligence is required, involving the following:

- Submission of the original of a document as defined in Section 4(4) of the Money Laundering Act (passport, ID card, etc.);
- Submission of a certified copy of such a document; or
- Presentation of a qualified digital signature as defined in Section 2 of the Digital Signature Act. In this case, the institution is required to check the validity of the certificate, the certification service provider report in accordance with Section 4(3) of the Act, the integrity of the certificate, and its relation to the signed data.

619. In addition, in all such cases, the Act requires that the first transaction must be carried out through another account opened in the contracting party's name with a credit institution covered by the Third EC Money Laundering Directive or a credit institution in a non-EU country subject to requirements equivalent to those of the EU Member States' 'equivalence list' published by the BaFin. Section 6(3) of the Act provides that the authorities may, by statutory instrument, impose additional requirements to address the higher risks associated with non-face-to-face business, but no such additional measures have yet been introduced.

#### *Effectiveness of implementation (of overall CDD measures)*

620. The above analysis identifies a number of specific areas where implementation of the measures, relative to the FATF standards, is problematic. These include the very broad exemption granted with respect to "low-risk" customers; the treatment of the EU member states and the third country equivalence list as the basis for a single risk category when determining certain low-risk scenarios; the application of the principle that the EU is a single domestic market in terms of the correspondent banking obligations; and the concept of what constitutes "senior management" in relation to the approvals process for PEPs and correspondent banking relationships. However, these are structural issues resulting from the legal and regulatory framework specified by the authorities, and there is no evidence to suggest that the institutions are, in general, doing less than is required of them. One area of particular concern that falls outside this category is the verification of beneficial ownership (including the determination of whether the beneficial owner might be a PEP). As indicated in the above analysis, there appears to be a wide variety of interpretations of what is expected under the risk-based approach provided under the new AML Act. The overall impression is that, whichever approaches are being adopted by individual institutions on the basis of their understanding of the law, they do not comply with the FATF requirements, which specifies that reasonable measures must be taken in all cases to verify the identity of the ultimate beneficial owner. The clarification issued by the BaFin in July 2009 may assist on this issue.

621. More generally, discussions with the larger financial institutions suggest they appear to have a high level of appreciation of their obligations under the AML Act. Whether this extends to the small regional and community banks, is more difficult to assess. The BaFin reports that the substantial work undertaken annually by the external auditors (see section 3.10 below), and its own analysis, has failed to register any systemic problems. However, it has to be noted that the new AML legislation only came into force in August 2008, and thus it may be too early to establish clearly that there are no widespread problems, particularly in respect of implementation of the risk-based measures; but it has to be taken into account, that even before the new AML legislation came into force some elements of a risk-based approach have been included within the German AML/CFT regulations. Some institutions (particularly those

without significant international experience) conceded that the risk-based approach is a difficult area for them in developing appropriate systems and controls.

### 3.2.2. *Recommendations and Comments*

622. In order to comply fully with Recommendations 5, 6, 7 and 8, Germany should:

#### *With respect to Recommendation 5:*

- Clarify the obligation with respect to the verification of beneficial ownership to bring it in line with the FATF standard, which requires that reasonable measures be taken to verify such ownership in all cases, including low risk.
- Extend the concept of beneficial ownership of trusts and *Treuhand* to include the settlor and any additional parties who may have direct or indirect control over the administration of the trust.
- Review the exemption for low-risk customers and transactions to ensure that:
  - The types of counterparty and the countries of origin are based on an appropriate risk-assessment by the authorities;
  - There remains an absolute obligation to monitor business relationships with such customers on an ongoing basis, and to keep records and information up to date; and
  - The exemption does not apply to circumstances where an institution has doubts about the veracity of information in its possession.
- Require institutions to consider filing an STR in case of failure to complete CDD.
- Review the timeframe (2-10 years) in which institutions are expected to apply the current CDD requirements to existing customers.

#### *With respect to Recommendation 6:*

- Introduce an explicit requirement that the enhanced due diligence requirements apply in the event that a PEP is the beneficial owner of the contracting party.
- Redefine the concept of a PEP to ensure that it does not exclude foreign PEPs who are resident in Germany.
- Require “senior level” approval for establishment (and continuation) of a business relationship with a PEP, rather than simply the next level of management.

#### *With respect to Recommendation 7:*

- Extend the special enhanced CDD measures to respondent banks within the European Union.
- Require “senior level” approval for establishment of a correspondent banking relationship, rather than simply the next level of management.

**With respect to Recommendation 8:**

- Introduce a specific obligation to have measures in place to prevent the misuse of technological developments.

**3.2.3 Compliance with Recommendations 5 to 8**

	Rating	Summary of factors underlying rating
R. 5	PC	<ul style="list-style-type: none"> <li>• Reasonable measures to verify beneficial ownership are not required in all cases.</li> <li>• Definition of beneficial ownership of a trust is incomplete.</li> <li>• Broad exemptions from CDD given for “low-risk” customers without apparent risk assessment.</li> <li>• “Low-risk” exemptions result in absence, in certain circumstances, of any obligation (i) to undertake ongoing monitoring of transactions and (ii) to undertake CDD when doubts arise about the veracity of existing customer identification.</li> <li>• No requirement to consider filing STR in case of failure to complete CDD.</li> <li>• No clear evidence of the overall level of implementation due to relatively recent enactment of new obligations.</li> </ul>
R. 6	PC	<ul style="list-style-type: none"> <li>• No requirements with respect to PEPs when they are the beneficial owners of the contracting party.</li> <li>• Provisions do not apply to foreign PEPs residing in Germany.</li> <li>• Approval to commence or continue the business relationship is not specified to be at senior management level.</li> </ul>
R. 7	PC	<ul style="list-style-type: none"> <li>• Special measures apply only to non-EU correspondent relationships.</li> <li>• Approval to commence the business relationship is not specified to be at senior management level.</li> </ul>
R. 8	LC	<ul style="list-style-type: none"> <li>• No specific obligation to take measures to prevent the misuse of technological developments.</li> </ul>

**3.3. Third Parties and Introduced Business (R. 9)****3.3.1. Description and Analysis****Legal Framework**

623. The AML Act distinguishes between two types of situation where third parties may be involved in the CDD process. The first consists of cases in which financial institutions transfer the task of fulfilling some or all elements of CDD (except for ongoing supervision of business relationships) to other third parties on the basis of a contractual agreement. This amounts to outsourcing, and the measures taken by the third party are legally attributable to the institution (Section 7(2) of the Act). Such arrangements fall outside the scope of Recommendation 9, but it may be noted that this type of arrangement was commonplace in Germany prior to the introduction of the non-face-to-face provisions in the new AML Act. An arrangement exists whereby Deutsche Post can carry out the verification of identity on behalf of the banks (through its PostIdent facility), and communicate the results and supporting documentation directly to the relevant bank through an electronic link.

624. The second and more general situation, which falls under the scope of Recommendation 9, is under Section 7(1), which permits financial institutions to rely upon specified third parties to perform certain of the due diligence requirements laid down in Section 3(1) of the Act, specifically in relation to the identification and verification of the contracting party and the beneficial owner. The obligation, under Section 3(1) number 4, to undertake ongoing monitoring of the business relationship cannot be delegated to a third party.

***Requirement to Immediately Obtain Certain CDD elements from Third Parties (c. 9.1); Availability of Identification Data from Third Parties (c. 9.2)***

625. Section 7(1) requires that third parties must immediately forward to the financial institution the information gathered in fulfilling the equivalent measures to those laid down in Section 3(1) of the Act (*i.e.* the CDD measures); and that, at the request of the financial institution, they must also forward copies of identification data and other relevant documentation on the identity of the contracting party or the beneficial owner. It has to be noted that the legislation (in following the structure of the Third EC Money Laundering Directive) imposes these obligations directly on the third party (who may well be outside German jurisdiction), and there is no explicit requirement to indicate that the responsibility should lie with the financial institution to satisfy itself that the third party will comply with the request for the relevant information. The authorities have indicated that, by imposing the obligation onto the third party, there is an implicit obligation on the German institution to satisfy itself that the third party will be able and willing to fulfill its responsibilities. While this may be a reasonable presumption, there appears to be no compelling reason why the approach adopted here should be different from the direct obligation imposed on financial institutions when dealing with their other customers.

***Regulation and Supervision of Third Party (applying R. 23, 24 & 29, c. 9.3); Adequacy of Application of FATF Recommendations (c. 9.4)***

626. Section 7(1) defines the types of third party upon whom reliance may be placed, based primarily on an equivalence test. These expressly include credit institutions, financial services institutions, insurance undertakings, insurance intermediaries, lawyers, auditors, chartered accountants, tax advisers and tax agents established in all EU member states; but exclude money transmission services providers and currency exchange businesses. In addition, the list extends, on a discretionary basis, to credit institutions, lawyers, notaries, auditors, tax advisers and insurance undertakings based in non-EU countries, if

- They conduct business covered by the Third EC Money Laundering Directive or provide accident insurance with premium redemption;
- They are subject to mandatory registration or authorization;
- They apply due diligence requirements and record-keeping requirements equivalent to those laid down in the Third EU Money Laundering Directive; and
- They are supervised accordingly.

627. Where the introduction is made through a separately incorporated business entity in the same group as the financial institution, the overall requirements still apply. In the case of foreign branches, these are regarded as integral parts of the financial institution, and not as third parties.

628. These categories of eligible third-party introducers are clearly defined by statute (the list being based on the collective view within the EU that such professions can usually be relied upon to undertake appropriate due diligence), and, in principle, an institution need not undertake any qualitative assessment



when relying on a third-party based in the EU. In identifying those non-EU third countries fulfilling the specified requirements, the authorities expect financial institutions to rely firstly upon the European Union's member states' "equivalence list", and secondly upon the result of the country assessments undertaken by the FATF, FSRBs, IMF and World Bank. According to Section 7 (3) of the Act, the competent Federal Ministry may, in order to implement a decision of the European Commission, determine that financial institutions may not rely on other third parties located in certain jurisdictions outside the EU. However, no such regulation has been issued to date.

629. In practice, it was clear, from discussions during the assessment mission, that there was a presumption that, because the BaFin has issued the EU "equivalence list," all jurisdictions on this list (including the non-EU members of the FATF) are officially deemed to meet the relevant criteria. However, no independent risk assessment had been undertaken by the authorities prior to issuing the list, although it resulted from the collective views of the EU member states. While this procedure is largely implementing a provision within the Third EC Money Laundering Directive, it has to be noted that this particular provision is entirely discretionary within the Directive. In July 2009, the BaFin issued circular 14/2009, in which it states that the general presumption that institutions established in other EU member states, or in jurisdictions on the equivalence list, undertake CDD obligations to a level equivalent to those expected in Germany could be overruled by information to be found in the results of the country assessments undertaken by the FATF, FSRBs, IMF, and World Bank. This is important clarification, especially given that the range of institutions and professions on which reliance may be placed is very broad and extends well outside the financial sector. However, there remains the risk that, unless the institution is proactive in searching for such negative information, it will assume that reliance may reasonably be placed on the geographical scope of introducers specified in the statute.

#### ***Ultimate Responsibility for CDD (c. 9.5)***

630. Section 7(1) specifies that, while reliance may be placed on third parties in the defined circumstances, the ultimate responsibility for meeting the CDD requirements in general remains with the institution covered under the Act.

#### ***Effectiveness of implementation***

631. The general perception among the mainly larger financial institutions with which the assessors met was that, while the concept of third-party introduced business is important to them, they consider that the list of equivalent jurisdictions is excessively broad and does not coincide with their own risk assessments. For instance, an application of the principles within the AML Act would permit reliance legal professionals in two offshore financial centers included within the equivalence list through their association with FATF member countries, even though the general message from the authorities is that such centers pose a *prima facie* high risk. Therefore, institutions have a tendency to apply a much more cautious approach to EU and third-country introductions than permitted under the AML Act. The assessors are not in a position to determine the practice in the much wider range of smaller institutions, although their use of this facility is likely to be very limited, given the very localized nature of their business.

#### ***3.3.2. Recommendations and Comments***

632. In order to comply fully with Recommendation 9, Germany should implement a procedure to review the range of third party introducers and the composition of the EU equivalence list to ensure that it accurately reflects the authorities' own assessment of the risks.

### 3.3.3. Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9	LC	<ul style="list-style-type: none"> <li>No national assessment of the suitability of the specified institutions and professions which may act as introducers.</li> </ul>

## 3.4. Financial Institution Secrecy or Confidentiality (R.4)

### 3.4.1. Description and Analysis

#### *Legal Framework*

633. German credit institutions generally have an obligation to maintain the confidentiality of the information that they acquire in the course of their business relationships. There is, however, no specific legal provision on banking secrecy. The confidentiality requirement is not set out in law, but is in the contract between the bank and its clients. It is usually included in the bank's General Terms and Conditions of Business (GTCB) and is a secondary obligation of the contractual relationship between the bank and its customers. The most commonly used GTCB are those that were established by the five banking associations for their members ("GTCB for Banks"), and received the approval of the Federal Cartel Office. These have been adopted by most of the banks in Germany and reflect the general practice, but are not mandatory as such, and the banks may choose to stipulate other conditions. Section 2 (1) of the GTCB for Banks stipulates that a bank may depart from the contractual confidentiality obligation in three cases, when:

- The bank is obliged by law to provide customer information,
- The customer consents to the disclosure, or
- The bank is allowed to disclose customer information.

634. While Section 203 of the CC punishes the violation of "private secrets" by a number of authorities, businesses, and professions, it does not apply to credit institutions. Breaches of banking confidentiality are, therefore, not sanctioned by criminal laws and can only be raised in the course of civil proceedings.

#### *Inhibition of Implementation of FATF Recommendations (c. 4.1)*

##### *Access to information by relevant authorities*

635. The confidentiality requirement must generally be observed towards the authorities but there are circumstances in which it is overridden by specific legal requirements for disclosure.

636. Banking confidentiality does not apply where there is a public law obligation to provide information to authorities duly authorized to request it. This includes information requested by the BaFin and the *Bundesbank* in the context of supervision (Section 44 (1) of the Banking Act). The only grounds for refusal to provide the BaFin with requested documentation and information are the private grounds listed in the CPC (*i.e.* when disclosure places the requested person and/or his or her relatives at risk of criminal prosecution or proceedings under the Act on breaches of administrative regulations (Section 44(6) of the Banking Act). Banking confidentiality is not a valid obstacle to disclosure.

637. In order to comply with their reporting obligations (see Section 3.7 below), credit institutions must provide the relevant information, including information on the customer and his or her accounts, to the competent authorities, and may not refuse to file STRs on the grounds of banking secrecy. Section 13 of the Act explicitly releases anyone who reports these facts from any civil or criminal liability, unless the reporting was made in a deliberately or grossly negligently false way. This provision protects the credit institutions against potential claims for breach of confidentiality when a report was made in good faith.

638. In the course of criminal proceedings, credit institutions must, if requested, give evidence to the courts and to the public prosecutor. They may be called upon as witnesses and may not refuse to testify on professional secrecy grounds (Section 53 of the CPC explicitly lists those who may refuse to testify on professional secrecy grounds but does not mention credit institutions).

639. As mentioned in the discussion of Recommendation 28, prosecutors and law enforcement agencies have direct powers to compel the production of information held by the general public. They can also compel other authorities (such as the BaFin, for example) to produce information that they may have. They can also request the competent court to issue an order enabling them to search premises (including private premises) and seize all the necessary information and documents in the context of a criminal investigation. The Federal Office for the Protection of the Constitution may also, if there are actual indications of particular terrorist undertakings, request information from credit institutions, financial services institutions, and finance companies in relation to accounts, account holders and other beneficiaries, other parties involved in payment transactions, and cash movements and investments (particularly account balances and incoming and outgoing payments).

#### **Exchange of information between relevant authorities**

640. The use by the authorities of STR information is limited by law. According to Section 11(6) of the AML Act, the content of an STR may only be used for criminal proceedings relating to ML, TF and a criminal offense liable to maximum punishment of more than three years of imprisonment, for taxation proceedings, for the supervisory tasks of competent authorities, and for the purpose of threat prevention. This limitation ensures that the information provided with the STR remains in the hands of the competent law enforcement agencies' authorities, without limiting the exchange of information between them.

641. In certain circumstances, the BKA or the FIU, or both may transmit personal data to other authorities and other public-sector entities, such as the BaFin (Section 10 of the Federal Criminal Police Office Act in conjunction with Section 10 of the AML Act). The FIU may also cooperate with their foreign counterparts and provide banking information contained in an STR.

642. In the exercise of its supervisory function, the BaFin may request information which has already been provided to another competent agency by addressing a request directly to that agency (Section 44(2a) of the Banking Act).

#### **Exchange of information between credit institutions as required by R. 7, R. 9 and SR VII**

643. There are no provisions that prevent institutions from complying with the obligations listed under Recommendations 7 and 9, and Special Recommendation VII. Provided that it is used solely for the purpose of preventing ML and TF, institutions may exchange information on STRs with other institutions within the same group or holding, as well as with institutions in Germany or in other EU members or third countries subject to similar requirements as those set out in the Third EC Money Laundering Directive, without this constituting a violation of the prohibition of tipping-off (Section 12(1) of the AML Act).

***Effectiveness of implementation:***

644. Banking secrecy does not inhibit the implementation of the FATF Recommendations by the authorities. The law enforcement, FIU and supervisory authorities have sufficient legal basis to request access to information held by credit institutions to fulfill their respective functions and, in practice, none of the authorities encountered raised any difficulty in obtaining that information. Credit institutions are aware of their obligations to disclose information when the conditions for disclosure are met and cooperate with the authorities in this respect. The authorities informed the assessors that they are satisfied that the current framework enables them to obtain all necessary information and that the banking secrecy does not constitute an obstacle.

***3.4.2. Recommendations and Comments***

None

***3.4.3. Compliance with Recommendation 4***

	Rating	Summary of factors underlying rating
R.4	C	This Recommendation is fully observed.

**3.5. Record-keeping and wire transfer rules (R.10 & SR.VII)*****3.5.1. Description and Analysis******Record-Keeping & Reconstruction of Transaction Records (c. 10.1 & 10.1.1); Record-Keeping for Identification Data, Files and Correspondence (c. 10.2)***

645. According to Section 8(1) of the AML Act, all data collected and information gathered in fulfilling the requirement to perform due diligence (regardless of whether it was pursuant to Section 3(1) of the AML Act or in cases of simplified or enhanced due diligence) on contracting parties, beneficial owners, business relationships, and transactions must be recorded. According to Section 8(3), these records and other evidence pertaining to business relationships and transactions must be kept for at least five years, without prejudice to other legal provisions (for example, Section 257 of the Commercial Code, described below). With regard to information on business relationships (including transactions), the retention period must begin at the end of the calendar year in which the business relationship was terminated. In all other cases (in particular one-off transactions), it must begin at the end of the calendar year in which the information was obtained.

646. In addition, for all other documents, including contractual correspondence, the duty on the part of financial institutions to record and retain documents follows from the general duties contained in Section 257 of the Commercial Code. This requires all “merchants” (including financial institutions) conducting commercial transactions to retain specific records and to furnish information on demand. These include the following:

- Books of account, inventories, opening balances, management reports, annual accounts, corporate accounts, corporate management report and all working instructions necessary for their understanding as well as further organizational documents;
- Any trade letters received (documents concerning a trading transaction);

- Copies of trade letters dispatched; and
- Receipts for bookings in the records which must be kept according to Section 238(1) of the Commercial Code (booking receipts).

647. The documents specified in the first and fourth bullets have to be retained for 10 years; the other documents specified in the second and third bullets for six years (Section 257(4) of the Commercial Code). The period of storage commences with the end of the calendar year in which the entry into the book of account was made, the inventory was compiled, the opening balance or the annual account was ascertained, the corporate account was compiled, the trade letter was received or dispatched, or the booking receipt was generated (Section 257(5) of the Commercial Code).

648. According to EU Regulation 1781/2006 on wire transfers, the payment service provider must keep records of complete information on the payer which accompanies transfers of funds for five years (Article 5(5) of the Regulation) and the payment service provider of the payee must keep records of any information received on the payer for five years (Article 11 of the Regulation).

649. Finally, there are additional specific duties for credit institutions and financial services institutions in the tax and regulatory laws. The first arises from Section 154(2) of the Fiscal Code, read in conjunction with number 6 of the Fiscal Code Application Ordinance on Section 154. This duty obliges credit institutions to record the data established on the opening of an account, securities account or the allocation of a safe deposit box and to retain it for a period of five years. The second is contained in Section 25a(1) of the Banking Act and requires credit institutions and financial services institutions to have in place a proper business organization which must, among other things, cover complete documentation of the business activity in order to enable overall supervision by the BaFin. The relevant records have to be kept for at least five years.

#### ***Availability of Records to Competent Authorities in a Timely Manner (c. 10.3)***

650. Section 8(2) of the AML Act requires that all records are accessible during the retention period and “can be made available at any time for reading, given reasonable advance notice.” In the BaFin’s 1998 circular (which has been repealed but which still reflects the BaFin’s administrative practices, in as far as it does not conflict with the new law or industry practice), institutions are instructed that, in order to meet requests for information from law enforcement, “the records or copies of identification documents made are to be filed in alphabetical order on a yearly basis to guarantee clear allocation. In the case of computer-based data records, it suffices that alphabetic traceability is guaranteed.” It goes on to state that “high standards must be set for the legibility of the records to be kept under the Money Laundering Act.” In addition, Section 8(4) of the AML Act provides that, where records subject to retention must be presented to a public agency (for example, a supervisory or a law enforcement agency), Section 147(5) of the Fiscal Code applies, as appropriate. This last provision sets down the basis and format in which certain records are to be stored for easy retrieval. Section 25a(1) of the Banking Act requires that all information held by financial institutions must be made available readily to the BaFin.

#### ***Wire transfers: legal framework***

651. The European Union’s Regulation 1781/2006 implements SRVII throughout the European Union. The Regulation applies directly to its addressees, without further implementation being required by member states through their national legislatures. However, at the national level, supplementary provisions exist in order, first, to determine the competent authorities for the supervision of payment services providers’ (PSPs) compliance with the Regulation, and second, to create provisions for sanctions against violations of its provisions.

652. According to Article 3, the Regulation applies to transfers of funds, in any currency, which are sent or received by a PSP established in the EU. However, it does not apply in the following cases:

- Transfers of funds carried out using a credit or debit card, provided that:
  - (a) The payee has an agreement with the PSP permitting payment for the provision of goods and services; and
  - (b) A unique identifier, allowing the transaction to be traced back to the payer, accompanies such wire transfer (Article 3(2) of the Regulation).
- Transfers of funds using electronic money covered by that derogation, except where the amount transferred exceeds EUR 1 000 (USD 1 392) (Article 3(3) of the Regulation).
- Transfers of funds carried out by means of a mobile telephone or any other digital or Information Technology (IT) device, when such transfers are pre-paid and do not exceed EUR 150 (USD 209) (Article 3(4) of the Regulation)
- Transfers of funds carried out by means of a mobile telephone or any other digital or IT device, when such transfers are post-paid and meet all of the following conditions:
  - (a) The payee has an agreement with the PSP permitting payment for the provision of goods and services;
  - (b) A unique identifier, allowing the transaction to be traced back to the payer, accompanies the wire transfer; and
  - (c) The PSP is subject to the obligations set out in the Third EU Money Laundering Directive (Article 3(6) of the Regulation).
- Transfers of funds:
  - (a) Where the payer withdraws cash from his or her own account;
  - (b) Where there is a debit transfer authorization between two parties permitting payments between them through accounts, provided that a unique identifier accompanies the wire transfer, enabling the natural or legal person to be traced back;
  - (c) Where truncated checks are used;
  - (d) To public authorities for taxes, fines or other levies within a Member State; and
  - (e) Where both the payer and the payee are PSPs acting on their own behalf.

653. Against this background, all credit institutions in Germany carrying out Giro business (Section 1(1) number 9 of the Banking Act) and financial service institutions carrying out money transmission services (Section 1(1a) number 6 of the Banking Act) fall under the scope of Regulation 1781/2006.



***Obtain Originator Information for Wire Transfers (applying c. 5.2 & 5.3 in R.5, c.VII.1)***

654. According to Article 5 of Regulation 1781/2006, the payer's PSP has to ensure that transfers of funds are accompanied by complete information on the payer. Article 4 defines 'complete information' as consisting, in principle, of the name, address, and account number. The address may be substituted with the date and place of birth of the payer, a customer identification number or national identity number. Where the payer does not have an account number, the PSP has to substitute it with a unique identifier which allows the transaction to be traced back to the payer.

655. Under Article 5(2), the PSP, before transferring the funds, has to verify the complete information on the payer on the basis of documents, data or information obtained from a reliable and independent source. This provision does not apply where the value of the transfer is less than EUR 1 000 (USD 1 392), unless the transaction is carried out in several smaller transactions that appear to be linked. For verification purposes the provisions of Section 4(4) of the AML Act apply, which means that the PSP has to use the following documents:

- For natural persons: valid official identity card including the holder's photograph which satisfies domestic requirements for identity cards or passports, in particular domestic passports and passports, identity cards or their substitutes recognized or accepted under legislation concerning foreigners; and
- For legal persons or partnerships: a copy of the relevant entry in the commercial register or register of cooperative societies or similar official register; foundation charters or equivalent documents; or access to the register data.

656. Article 5(3) of the Regulation states that verification may be deemed to have taken place, if:

- a) A payer's identity has been verified in connection with the opening of the account and the information obtained by this verification has been stored in accordance with the obligations set out in Articles 8(2) and 30(a) of the Third EC Money Laundering Directive; or
- b) The payer falls within the scope of Article 9(6) of the Third EC Money Laundering Directive (*i.e.* he/she is a customer who existed prior to the implementation of the Directive's provisions, but has been subject to verification on a risk-based approach).

657. According to Article 5(5), the payer's PSP has to keep records of the complete information on the payer for five years. Under Article 14, the PSPs of both the payer and the payee have to respond fully and without delay to requests for relevant information made by competent authorities.

***Inclusion of Originator Information in Cross-Border Wire Transfers (c. VII.2)***

658. According to Article 7(1) of the Regulation, transfers of funds where the payer's PSP is situated outside the European Union must be accompanied by complete information on the payer (as defined). Transfers from one European Union Member State to another Member State are not considered to be cross-border for the purposes of the Regulation, and, therefore, this provision does not apply in such circumstances. For the purposes of SRVII, the FATF has recognized that transfers within the EU may be treated as domestic transactions, and therefore this limitation is not considered to be a deficiency in this case (cf. comments under Recommendation 9, etc.). Although the text of the Regulation is not specific on this point, the authorities indicated that, any transfer that involves an initial intermediary in the EU before being passed to a third country, would have to be treated as a cross-border transaction by the initial payer's PSP.

659. In the case of batch file transfers from a single payer where the payees' PSPs are situated outside the European Union, Article 7(1) of the Regulation does not apply to the individual transfers bundled together, provided that the batch file contains that information and that the individual transfers carry the account number of the payer or a unique identifier.

***Inclusion of Originator Information in Domestic Wire Transfers (c. VII.3)***

660. Article 6(1) of the Regulation stipulates that in cases where both the PSPs of both the payer and the payee are situated in the European Union, transfers of funds may be accompanied only by the account number of the payer or a unique identifier allowing the transaction to be traced back to the payer. Under Article 6(2) of the Regulation, the payee's PSP has the right to request and to obtain complete information on the payer within three working days after the request.

***Maintenance of Originator Information ("Travel Rule") (c.VII.4)***

661. Under Article 12 of the Regulation, an intermediary PSP is required to ensure that all information received on the payer is maintained with the transfer.

662. According to Article 13(1) and (2), an intermediary PSP, when receiving a transfer of funds from a payer's PSP outside the European Union, may use a payment system with technical limitations which prevent information on the payer from accompanying the transfer of funds to send transfers of funds to the payment service provider of the payee, unless the intermediary PSP becomes aware that information on the payer required under this Regulation is missing or incomplete. If the latter applies, the intermediary PSP may only use a payment system with technical limitations if it is able to inform the payee's PSP of this fact, either within a messaging or payment system, or through another procedure, provided that the manner of communication is accepted by, or agreed between, both PSPs (Article 13(3)).

663. In cases where the intermediary PSP uses a payment system with technical limitations, the intermediary PSP has to make available to the payee's PSP, upon request, all the information on the payer which it has received, irrespective of whether it is complete or not, within three working days of receiving that request (Article 13(4)). The intermediary PSP has to keep records of all information received for five years (Article 13(5)), as does the payee's PSP (Article 11).

***Risk-Based Procedures for Transfers Not Accompanied by Originator Information (c. VII.5)***

664. Under Article 8 of the Regulation, the payee's PSP has to detect whether, in the messaging or payment and settlement system used to effect a transfer of funds, the fields relating to the information on the payer have been completed using the characters or inputs admissible within the conventions of that messaging or payment and settlement system. Such provider must have effective procedures in place in order to detect whether the following information on the payer is missing:

- a. For transfers of funds where the payer's PSP is situated in the European Union, the information required under Article 6 of the Regulation;
- b. For transfers of funds where the payer's PSP is situated outside the European Union, complete information on the payer as referred to in Article 4, or where applicable, the information required under Article 13 of the Regulation; and
- c. For batch file transfers where the payer's PSP is situated outside the European Union, complete information on the payer as referred to in Article 4 of the Regulation in the batch file transfer only, but not in the individual transfers bundled therein.

665. According to Article 9, if the payee's PSP becomes aware, when receiving transfers of funds, that complete information on the payer is missing or incomplete, it must either reject the transfer or ask for complete information on the payer. Under Article 10, the payee's PSP has to consider missing or incomplete information on the payer as a factor in assessing whether the transfer of funds, or any related transaction, is suspicious, and whether it must be reported to the authorities responsible for combating ML or TF; in the case of Germany; the law enforcement agencies and the FIU (Article 9(3)).

666. Where a PSP regularly fails to supply the required information on the payer, the payee's PSP must take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that PSP or deciding whether or not to restrict or terminate its business relationship with that PSP (Article 9(2)). In such circumstances, the payee's PSP has to report that fact to the competent authorities (Article 9(3)).

667. To provide specific guidance on these obligations under Articles 8 and 9, the BaFin has uploaded the Guidance entitled "Consultation on common understanding of the obligations imposed by European Regulation 1781/2006 on the information on the payer accompanying funds transfers to PSPs of payees" to its webpage. This Guidance was developed and published by the Anti-Money Laundering Task Force, a common Working Group of the Three Level 3-Groups of European Financial Supervisors (CEBS, CEIOPS and CESR), in October 2008.

#### ***Monitoring of Implementation (c. VII.6)***

668. According to Article 15(3) of the Regulation, EU member states have to appoint competent authorities to effectively monitor, and take necessary measures with a view to ensuring, compliance with the requirements of the Regulation. Germany has implemented this provision in Section 25b of the Banking Act by specifying that the "BaFin supervises the compliance with the obligations contained in Regulation 1781/2006 by credit institutions and financial services institutions performing money remittance services according to Section 1(1a), second sentence, number 6 of the Banking Act." Besides exercising its own authority, the BaFin makes use of the institutions' annual audit reports, which, under Section 29(2) of the Banking Act, have to contain statements explaining whether the institution has observed its obligations under the Money Laundering Act, including those under the obligations contained in Regulation 1781/2006.

#### ***Application of Sanctions (c. VII.7: applying c.17.1 – 17.4)***

669. Article 15(1) of the Regulation obliges member states to lay down rules on effective, proportionate and dissuasive penalties applicable to infringements of the provisions of the Regulation, and to take all measures necessary to ensure that they are implemented. In Germany, under Section 56(4) of the Banking Act, an administrative offense is deemed to have been committed by anyone who contravenes Regulation 1781/2006, intentionally or by negligence, in one of the following ways:

1. By failing to ensure that transfers of funds are accompanied by complete information on the payer, in violation of Article 5(1) of Regulation 1781/2006;
2. By failing to verify the complete information on the payer or to do so in a timely fashion, in violation of Article 5(2) also in conjunction with (4) of Regulation 1781/2006;
3. By failing to ensure that transfers of funds are accompanied by complete and accurate information on the payer, in violation of Article 7(1) of Regulation 1781/2006;
4. By failing to have effective procedures in place in order to detect whether the required information on the payer is missing, in violation of Article 8, second sentence, of Regulation 1781/2006;

5. By failing to reject the transfer or ask for complete information on the payer, or to do either in a timely fashion, in violation of Article 9 (1), first sentence, of Regulation 1781/2006;
6. By failing to keep records of any information received on the payer for at least five years, in violation of Articles 11 or 13(5) of Regulation 1781/2006; and
7. By failing to ensure that all information received on the payer that accompanies a transfer of funds is kept with the transfer, in violation of Article 12 of Regulation 1781/2006.

670. The BaFin is the competent administrative authority for applying such administrative sanctions within the meaning of Section 36(1) number 1 of the Act on Administrative Offenses (Section 60 of the Banking Act). The penalty for such offenses is a payment of up to EUR 50 000 (USD 69 585), but no sanctions have yet been applied.

***Additional elements: elimination of thresholds (c. VII.8 and c. VII.9)***

671. There are no thresholds, under Regulation 1781/2006, with respect to the need for full and accurate originator information on both inbound and outbound transfers.

***Effectiveness of implementation***

672. Given the plethora of different legal requirements relating to the retention of records generally, the authorities indicated that many institutions, particularly those in the banking industry, have decided for practical reasons to go over to the practice of keeping all records for the longer retention period of ten years. The overall requirements are a very long-standing feature of German commercial law, and there is no evidence to suggest that institutions fail in meeting their obligations. Indeed, extensive record-keeping is a well established practice generally. However, there is one area of doubt in view of the CDD exemptions that are provided for low-risk situations under Section 5 of the AML Act, whereby an institution is exempted from the provisions of Section 3(1) of the Act, which addresses the key CDD components of verifying the customer's identity, identifying the beneficial owner, obtaining information on the purpose and intended nature of the business relationship, and conducting ongoing monitoring of the relationship (see Section 3.2 above). It remains unclear what information a financial institution would acquire in such circumstances and what would, therefore, be available to the law enforcement agencies.

673. The authorities indicated that bank compliance with the wire transfers regulation is a specific area covered in the auditors' annual report on AML/CFT compliance, and that there had been no significant incidents of failure by institutions to apply the outward transfer requirements. However, there continue to be some outstanding issues with respect to inward transfers from some specific countries, but the audits suggest that institutions are handling these in line with the Regulation. There also appeared to be a general awareness of the obligations within the financial institutions, and there was no evidence that the required procedures are not being followed.

***3.5.2. Recommendations and Comments***

674. In order to comply fully with Recommendation 10, Germany should;
- Consider the potential consequences of the "low-risk" exemptions for the retention of meaningful information that can be made available to the competent authorities.

### 3.5.3. Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	LC	<ul style="list-style-type: none"> <li>Uncertainty about what information would be acquired (and therefore retained) on “low-risk” customers.</li> </ul>
SR.VII	C	This Recommendation is fully observed.

## 3.6. Monitoring of Transactions and Relationships (R.11 & 21)

### 3.6.1. Description and Analysis

#### *Special Attention to Complex, Unusual Large Transactions (c. 11.1); Examination of Complex & Unusual Transactions (c. 11.2); Record-Keeping of Findings of Examination (c. 11.3)*

675. Certain aspects of Recommendation 11 are captured within the following provisions:

- Section 3(1) number 4 of the AML Act, which requires all institutions covered by the Act to “continuously monitor the business relationship, including scrutiny of transactions undertaken throughout the course of that relationship, to ensure that the transactions being conducted are consistent with the institution’s or person’s knowledge of the contracting party and beneficial owner, if applicable, the business and risk profile, including, where necessary, the source of funds and ensure that the documents, data, or information are updated at appropriate intervals”;
- Section 25 c (2) of the Banking Act, which requires that credit institutions “shall operate and update appropriate data processing systems which enable them to recognize business relationships and individual transactions that should be regarded as suspicious or unusual on the basis of experience and knowledge generally and specifically available within the credit institution concerning methods of ML, TF, and fraudulent activity to the detriment of institutions. Where such activity is detected, it shall be investigated in the context of the ongoing business relationship and individual transactions in order to be able to monitor and assess the risk of these business relationships and transactions and to determine whether it constitutes suspicious activity”;
- Section 80d(1) of the Insurance Supervisory Act, which has a similar requirement to that in the Banking Act; and
- Section 6(5) of the Investment Act provides that Section 25c(2) of the Banking Act (described above) applies equally to investment firms.

676. The first provision addresses primarily the required monitoring procedures as part of the ongoing due diligence process, although it clearly contains an element designed to identify unusual and potentially suspicious transactions. However, the assessors doubt the practical application of this requirement in relation to the statutory “low-risk” customers, given the fact that institutions are specifically exempted from Section 3(1) number 4 (*i.e.* the monitoring obligation) in such cases. The provisions in the banking and insurance legislation are more direct, and are targeted specifically at those institutions involved in business and payment transactions of a volume and size that require more sophisticated systems. In particular, they oblige relevant institutions to monitor for, and undertake an analysis of, unusual transactions.

677. While these provisions go some way towards addressing the expectations of Recommendation 11, they do not contain two of the essential ingredients, which are specifically to require institutions to record in writing their analysis of those transactions that the monitoring systems identify; and to retain the analyses for five years, so that the competent authorities may have access to background on those transactions that do not prima facie reach the threshold of being considered suspicious, and therefore do not result in a report being made to the FIU.

***Special Attention to Countries Not Sufficiently Applying FATF Recommendations (c. 21.1 & 21.1.1)***

678. There are no specific provisions in the AML Act that address the requirement to give special attention to countries that do not sufficiently apply the FATF Recommendations. Instead, reliance is placed on the application of the risk-based approach by financial institutions, and, in particular, on the requirement of Section 6(1) of the AML Act that institutions must apply enhanced due diligence to high-risk situations.

679. Section 6 (2) specifies mandatory measures only with respect to PEPs and non-face-to-face business. However, the explanatory memorandum to this Section stresses that the cases referred to in the Act do not represent an exhaustive list of high-risk situations, and it goes on to state that “one category of high-risk cases requiring special attention is business relationships with contracting parties based in countries or regions known to have lower or insufficiently effective standards of ML prevention compared to the international standards.” In addition, Section 6(3) of the Act provides that the Federal Minister of the Interior may designate additional cases where enhanced due diligence should be required, but no such regulation has been issued so far within the context of the principles of Recommendation 21.

680. That said, the BaFin routinely publishes circulars with information pertaining to specific countries or territories with weaknesses in their AML/CFT regime. These have included statements relating to countries included within the FATF’s NCCT exercise, and more recently in relation to those jurisdictions that have been the subject of public statements issued by the FATF since 2008. In addition, in 2002, the BaFin issued a circular concerning the “Transdnstrian Moldavan Republic” and the risks posed for institutions that might have correspondent relations with banks licensed by the breakaway region. These circulars typically include specific instructions as to what the BaFin expects institutions to do in response to the information, including, for example, the application of:

- More stringent requirements for customer identification in the case of business and financial transactions with individuals or legal entities or companies;
- More stringent obligations to exercise due diligence in respect of business relationships, especially correspondent relationships; and
- More stringent control and reporting obligations for business relationships and financial transactions.

681. The enforceability of such instructions is discussed in the following section. On a more focused basis, the BaFin has applied *de facto* restrictions on transfers to certain jurisdictions by the money remitters. This was largely in response to the problem caused by the so-called “financial agents” typology, which is discussed in more detail under Recommendation 13 below.



***Examinations of Transactions with no Apparent Economic or Visible Lawful Purpose from Countries Not Sufficiently Applying FATF Recommendations (c. 21.2):***

682. With respect to transactions with such countries that appear to have no economic or visible legitimate purpose, there are no specific obligations to examine and retain a written record of the findings, beyond those contained within the general CDD obligations.

***Ability to Apply Counter Measures with Regard to Countries Not Sufficiently Applying FATF Recommendations (c. 21.3)***

683. Section 11(7) of the AML Act enables the BMI and the MoF to issue regulations specifying individual types of financial transactions which are deemed to be suspicious and reportable. The authorities have indicated that the rationale behind Section 11(7) mainly came from the discussion within the FATF on the possible range of effective countermeasures that jurisdictions might invoke against non-cooperating countries and territories. Based on this Section, a ministerial regulation can be issued to the effect that transactions from or to those countries must be treated as suspicious. However, up to the time of the on-site visit, no such regulations had been issued.

684. In addition, the BaFin may deal with institutions on the basis of Section 6 of the Banking Act (and a similar provision in the Insurance Supervisory Act), which specifies, among other things, that the:

- “BaFin shall counteract undesirable developments in the banking and financial services sector which may endanger the safety of the assets entrusted to institutions, impair the proper conduct of banking business or provision of financial services, or involve serious disadvantages for the national economy; and
- BaFin may, as part of its statutory mandate, issue orders to institutions and their managers that are appropriate and necessary to stop and prevent violations of regulatory provisions or to prevent or overcome undesirable developments at an institution which could endanger the safety of the assets entrusted to the institution or could impair the proper conduct of its banking business or provision of financial services....”

685. Section 6 of the Banking Act stipulates that it lies within the discretion of the BaFin what countermeasures it wishes to take, but the BaFin stated that, in using these provisions in relation to countries with poor AML/CFT systems, it would follow a step-by-step approach in line with the principles of administrative law, which requires that measures be suitable, necessary, and proportionate. Although it has not yet applied the full range of possible measures with respect to any particular jurisdiction, the BaFin stated that it would:

- Alert financial institutions to business relations or transactions with persons, companies or financial institutions from specified countries with few or no effective AML/CFT standards;
- Require the application of certain enhanced due diligence measures with respect to those business relations or transactions with persons, companies, or financial institutions from those countries;
- Require financial institutions to pay particular attention to respondent banks or transactions involving such countries or territories, and include appropriate lists of high-risk jurisdictions, NCCTs, or both in their internal AML/CFT systems; and

- Limit or prohibit business relationships or transactions with specified countries or persons in such countries.

686. In response to the notices issued by the FATF under its various international cooperation initiatives, the BaFin has issued circulars to the financial sector addressing the first three of the above steps, but has never moved to the final step of prohibiting institutions to undertake transactions with specific countries. While the BaFin circulars generally are not directly enforceable, in the case of the these particular notices, there is a traceable path to some form of enforcement under Section 6 of the Banking Act and similar provisions, given the specificity of the circulars with respect both to the jurisdictions concerned and to the actions expected of institutions. The BaFin stated that noncompliance with the circulars is an undesirable development according to Section 6(3) of the Banking Act and similar provisions, and that it would therefore cause supervisory action by the BaFin. However, there have been no enforcement actions or judicial decision to date to test this principle. In discussions with the financial institutions, it was apparent that they regard the BaFin circulars in this context as being instructions, which they ignore at their peril.

### *Effectiveness of implementation*

687. The statutory provisions relating to the requirements of Recommendation 11 are generally weak (and do not even implement the provisions of Article 20 of the Third EC Money Laundering Directive). However, generally, banking institutions are clearly expected, under the Banking Act, to have automated systems to help detect complex and unusually large transactions or unusual patterns of transactions. Only a few smaller institutions or institutions with very restricted businesses have refrained from establishing such automated system on the basis of criteria established by the BaFin, but they are still expected to have procedures relevant to the scale and nature of their business, and they are still required to have other systems in place to detect unusual or suspicious transactions. However, the assessors could not establish whether, irrespective of the legal framework, it was widespread practice to monitor for such transactions.

688. With respect to Recommendation 21, there are similar deficiencies in the legal provisions, but specific guidance has been provided to institutions in the form of the BaFin circulars, which highlight weaknesses in the AML/CFT regimes of other countries, typically (but not exclusively) in line with the public statements made by the FATF. From the discussions with the financial institutions with which the assessors met, it was apparent that they were alert to the risks posed by transactions or customers associated with such countries, and that this was built into their risk-based approach. Indeed, there was some evidence that the institutions took a harsher line on country risk than was being conveyed by the authorities (for example, they tended to find the EU equivalence list to be “counter-intuitive” in respect of some countries). However, the ultimate ability of the BaFin to enforce its administrative ladder of counter-measures with respect to transactions involving jurisdictions with weak AML/CFT regimes remains untested.

### **3.6.2 Recommendations and Comments**

689. In order to comply fully with Recommendations 11 and 21, Germany should:

#### *With respect to Recommendation 11*

- Introduce an explicit requirement that a written analysis should be undertaken, and recorded (for a period of at least five years), of all complex, unusually large transactions and unusual patterns of transactions that have no apparent economic or lawful purpose.
- Clarify what procedures are expected with respect to “statutory” low-risk customers.

**With respect to Recommendation 21**

- Require institutions to pay special attention to business relationships and transactions with persons from or in jurisdictions that do not sufficiently apply the FATF standard, employing their own risk analyses, in addition to placing reliance on the circulars issued by the BaFin.
- Introduce an explicit requirement that a written analysis should be undertaken, and recorded, of all such transactions.

**3.6.3 Compliance with Recommendations 11 & 21**

	Rating	Summary of factors underlying rating
R.11	PC	<ul style="list-style-type: none"> <li>• Uncertainty about the ability of institutions to monitor statutory “low-risk” customers effectively.</li> <li>• No obligation to record and retain an analysis of transactions that have no apparent or visible economic or lawful purpose.</li> </ul>
R.21	PC	<ul style="list-style-type: none"> <li>• No explicit obligation to pay special attention to relationships and transactions involving countries with inadequate AML/CFT standards.</li> <li>• No obligation to record and retain an analysis of transactions that have no apparent or visible economic or lawful purpose.</li> </ul>

**3.7. Suspicious Transaction Reports and Other Reporting (R.13-14, 19, 25 & SR.IV)****3.7.1. Description and Analysis****Legal Framework**

690. The reporting requirements are set out in Section 11 of the AML Act and apply uniformly to all financial institutions.

**Requirement to Make STRs on ML and TF to FIU (c. 13.1, 13.2, 13.5 & IV.1)**

691. The STR reporting obligation fails to meet the requirements of the FATF standards in several key areas. Section 11 provides that “regardless of the amount involved, institutions and persons covered by this Act, having established facts which permit the conclusion that an act pursuant to Section 261 of the CC [*i.e.* the ML offense] or terrorism financing has been or will be committed or attempted, must report these facts without delay either orally, by telephone, in writing, by email, or through electronic data transmission, to the responsible law enforcement authorities with copy to the BKA/FIU”<sup>61</sup>. The linkage of the obligation to the ML offense sets a more restricted trigger for reporting than is envisaged by the FATF

<sup>61</sup> The assessors and the authorities agreed to use this translation of the first sentence of Section 11 of the AML Act for the purposes of this assessment, rather than the one that features in the translation of the full AML Act (annex ...) because it reflects more closely the wording of the official text. The German text of the first sentence of Section 11 reads as follows: “*Ein Verpflichteter hat unabhängig von der Höhe der Transaktion bei Feststellung von Tatsachen, die darauf schließen lassen, dass eine Tat nach § 261 des Strafgesetzbuches oder eine Terrorismusfinanzierung begangen oder versucht wurde oder wird, diese unverzüglich mündlich, telefonisch, fernschriftlich oder durch elektronische Datenübermittlung der zuständigen Strafverfolgungsbehörde und in Kopie dem Bundeskriminalamt—Zentralstelle für Verdachtsanzeigen—anzuzeigen.*”

standard, which requires such reports to be filed with respect to the more general “proceeds of criminal activity.”

692. As regards the “evidential” basis upon which STRs are to be filed, there appears to be a considerable divergence of views about exactly what the law requires, and what institutions believe that they are being required to do by the authorities. A strict reading of the law sets a considerably higher threshold than the concept of “suspects or has reasonable grounds to suspect” contained in the FATF standards, in that it appears to require a high degree of certainty to trigger the reporting requirement. However, the authorities dispute this and indicate that the notion of mere suspicion has underlain the STR system in Germany for many years, and that this interpretation is supported by the explanatory memorandum to the AML Act, which states that Section 11 is to be interpreted in line with the text of Article 22(1)(a) of the Third EC Money Laundering Directive, which requires member states to impose a reporting requirement when an institution “knows, suspects or has reasonable grounds to suspect that ML or TF is being or has been committed or attempted.” While this may well have been the intent of Section 11, the practical experience, as encouraged by the law enforcement authorities and understood by many institutions, strongly suggests that a high threshold for reporting is being applied. This issue is discussed at greater length in the analysis of effectiveness below.

693. As indicated, the obligation relating to ML is tied to the definition of the offense under Section 261 of the CC, which gives rise to two issues: first, the Section 261 offense is the act of ML itself (*i.e.* concealment of criminal proceeds) and so does not link the obligation directly to suspicions that funds are the proceeds of crime; and second, the definition of the predicate offenses for ML does not capture “insider trading and market manipulation,” nor “counterfeiting and piracy of products” among the list of necessary predicates defined by the FATF. With respect to TF, the definition within the AML Act also falls short of the FATF standard in that it does not cover the funding of individual terrorists or of specific terrorists acts. In principle, these limitations in the definitions have an impact on the scope of the STR obligation.

694. Federal German law (Constitution and the AML Act) requires that STRs be sent by reporting entities directly to the law enforcement agencies, with a copy to the federal FIU. The legislation provides that the reports may go to any police authority, but an agreement has been reached between the interested parties, such that the reports will go to respective *Länder* criminal police offices. In two *Länder*, the reports go directly to the public prosecutors’ office, rather than the police. In principle, this format may meet the standard expected under Recommendation 13 with respect to sending STRs to the FIU, although, as discussed under Recommendation 26, the FIU is not the central authority for analyzing and disseminating such reports. It appears also to be the case (from discussions with the financial institutions) that the decentralized reporting of the primary information to individual *Länder* authorities means that they have, on occasion, been required by the authorities to split an STR into separate reports in order to file each part with the relevant *Länder* authority. The position is further complicated with respect to the money services providers, who are also obliged, under an instruction issued in 1998, to file copies of the reports directly with the AML Unit of the BaFin in order to assist the unit with its supervisory responsibilities.

695. Failure to submit an STR is a specific offense under Section 17(1) number 4 of the AML Act. However, the offense relates only to circumstances where the failure was committed intentionally or with gross negligence. In cases where this standard of evidence could not be achieved, the BaFin would have to rely on its general administrative law procedures, as described under Recommendation 17. To date, there have been no sanctions applied for failure to report under either the new AML Act or its predecessor.

#### ***Requirement to Make STRs on TF to FIU (IV.1)***

696. As indicated above, the reporting obligation relates equally to TF, but is limited to the extent that the TF offense does not fully comply with the FATF definition. The following table, drawn from data in

the FIU's annual report, shows the number of filings specifically identified as being linked to TF or associated activities.

Activity	2008	2007	2006
Financing of terrorism	34	53	28
Matches with listed persons	22	28	21
Criminal association or organization	9	21	10

#### ***No Reporting Threshold for STRs (c. 13.3, c. IV.2)***

697. Section 11(1) of the AML Act specifically states that the reporting requirements apply to all suspicious transactions or attempted transactions regardless of the amount involved.

#### ***Making of ML and TF STRs Regardless of Possible Involvement of Tax Matters (c. 13.4, c. IV.2)***

698. Tax offenses, if committed on an organized or major scale, constitute predicate offenses to ML. Therefore, a possible involvement of tax matters in a suspicious transaction is not an obstacle to the reporting requirement.

#### ***Protection for Making STRs (c. 14.1)***

699. Under Section 13 of the AML Act, anyone who reports to the law enforcement authorities facts that suggest either a criminal offense pursuant to Section 261 of the CC, or TF "cannot be held responsible" for the report in question unless it has been made in a deliberately false or grossly negligent manner. The authorities have indicated that the notion of responsibility in this provision covers both criminal and civil liability. This provision also applies to any employee who reports suspicious activities to his or her supervisor or an in-house unit responsible for filing STRs.

#### ***Prohibition against Tipping-Off (c. 14.2)***

700. Section 12(1) of the AML Act prohibits the disclosure, to the person concerned or to any third party, of the fact that a report has been filed with the authorities. However, there is no provision that restricts disclosure of the fact that a suspicious transaction has been identified and that an STR is in the process of being prepared. The general prohibition is waived to permit institutions to share information among members of the same financial group, and between institutions that have a common interest in the transaction or the customer, provided that the other institution is in an EU member state or a third country deemed to have equivalent AML/CFT standards. This waiver is not in strict compliance with the FATF standard, which generally prohibits any disclosure to third parties other than the competent authorities. However, the FATF plenary has considered another EU member state's evaluation report that contained a similar waiver, and has concluded that the waiver is reasonable and represents a positive contribution to the overall effectiveness of the preventive measures.

701. Section 11(1) of the AML Act prohibits the execution of a suspicious transaction without the approval of the relevant state prosecutor, or within two working days of the report, if the prosecutor fails to respond within this time. This timescale is sufficiently short so as not to create a risk of inadvertent tipping-off. However, it is understood that it is common practice within the financial sector to suspend an account or to terminate a customer relationship once an STR has been filed. This is driven, in part, by the fact that institutions have a high degree of certainty that there is underlying criminal activity by the time that they file, and it is a practice that, according to the institutions, is not always welcomed by the law

enforcement authorities. This practice risks being a trigger for inadvertent tipping-off, but it was not something that the authorities believed caused particular problems in that respect.

702. More generally, the BaFin, which has responsibility under the AML Act for investigating potential cases of tipping-off, reported that there had been only a few investigations of alleged offenses under the new AML Act, although there had been a number of potential cases under the 2002 Act, largely due to the absence in that Act of the current provisions permitting intra-group disclosures of STRs.

***Additional Element – Confidentiality of Reporting Staff (c. 14.3)***

703. The information contained in an STR may be used only for criminal proceedings specified in Section 15(1) and 15(2) of the AML Act, for criminal proceedings related to a criminal offense liable to maximum punishment of more than three years imprisonment, for taxation proceedings, for the supervisory tasks of competent authorities pursuant to Section 16(2) of the Money Laundering Act, and for the purpose of threat prevention (Section 11(6) of the AML Act).

704. The names and personal details of persons who make an STR are granted special protection by the law enforcement agencies, as follows:

- STRs sent to the respective law enforcement agencies (and all information contained therein) automatically become part of the criminal investigation's case file. Access to this case file is restricted to a very limited number of persons, *e.g.* to the defence counsel or to other agencies upon application of an attorney showing the existence of a legitimate interest. The party charged with the offense has no right to inspect the file. The decision as to who will be granted access to the file rests with the public prosecutor's office during the preliminary investigation and after the criminal proceedings have been concluded by a final and binding judgment; otherwise, the decision rests with the court ruling on the matter.
- The personal data of parties submitting an STR are not stored at the FIU or at the State Criminal Police Offices in researchable files. The only information recorded is the designation of the party making the report (*e.g.* the name of the credit institution) and the reference number used by the party, but not the names of the ML officers. In addition, all FIU employees are under a general duty of confidentiality by virtue of their public office.

705. As an additional measure, the BaFin requires financial institutions to file STRs only through the ML compliance officer without disclosing the officer's name or the names of any members of staff of the financial institution involved in the respective case.

***Consideration of Reporting of Currency Transactions above a Threshold (c. 19.1)***

706. There is no general obligation to report all transactions in currency above a fixed threshold. The German legislature discussed the issue in November 1998 in the context of the implementation of the convention on drugs, and decided that the burden on the private sector would be excessive. The decision was reconfirmed during debate on both the 2002 and 2008 AML Acts.

***Feedback and Guidelines for Financial Institutions with respect to STR and other reporting (c. 25.2)***

707. Two types of feedback are provided to the reporting institutions. The first is supplied by the FIU in the form of the statistical analyses, typologies and emerging trends contained in its annual report and newsletters published on its website, which also includes references to information available from



international bodies such as Egmont and the FATF. The FIU also provides a secure access section on its website, which provides additional information of a more confidential nature.

708. Pursuant to Section 482(2) of the CPC, it is left to the individual state prosecutors to provide feedback on the fundamental quality and value of the STRs submitted by individual institutions within their region. Because each STR automatically generates a criminal investigation, there is provision within the CPC that permits an interested party to obtain information that was either submitted to the courts, or would have been submitted had a charge been brought. In criminal proceedings instituted on the basis of an STR, the responsible public prosecutor's office is obliged by Section 11(8) of the AML Act to inform the FIU about the charges and the outcome of the criminal proceedings. Responses from the public prosecutors' offices are collected at the FIU, recorded in a database and analyzed, with a view to assessing the significance of STRs for criminal prosecution, evaluating their forensic added-value, monitoring trends and typologies, and initiating or carrying out measures designed to optimize the reporting practice of the public prosecutors' offices. The FIU publishes these results in its Annual Report.

709. Throughout the meetings with the financial institutions, there was a recurrent theme that institutions felt that they were not receiving adequate or timely feedback on specific transactions, which would enable them to understand whether the reports had been of any value to the authorities. While they welcomed the data and analyses provided by the FIU, primarily through its annual reports, they recognized that the information that was of real operational and systemic value to them should be coming from the state prosecutors' offices, since they alone are responsible for the effective analysis and investigation of the reports. While performance will undoubtedly vary from state to state, the general sense was that significantly more should be done across-the-board to improve feedback. Some institutions felt that quality feedback was a fundamental issue for them in terms of the development of the STR regime.

710. The FIU has developed a model reporting form, which it has distributed to the reporting institutions. However, there is no obligation to use the form, although the FIU actively encourages its adoption, and the detailed nature of the STRs being filed by institutions seems to militate against its widespread use.

### ***Statistics (R.32)***

711. The FIU maintains and publishes in its annual reports comprehensive statistics on the STR regime, including numbers of STRs, sources, geographical distribution, underlying predicate offenses and investigations. A sample of these statistics is used in the following analysis of effectiveness of the system.

### ***Effectiveness of implementation***

712. As indicated in the above analysis of the legal provisions, there are serious doubts about the basis upon which institutions are being required to report. The assessors' view that the reporting threshold is far higher than suspicion or reasonable grounds to suspect is supported by two key indicators: the numbers of reports being filed, and the extent of the pre-filing analysis and investigation being undertaken by the institutions. These issues are each discussed below.

713. With respect to the numbers of STRs being filed by the financial sector, the following data are published by the FIU:

Statistical Table 20: STRs filed by the Financial Sector

		2008	2007	2006
<b>I. STRs submitted by financial sector institutions</b>				
Banks	Credit banks	2 102	2 147	2 882
	Savings banks and state central banks	2 495	2 810	3 072
	Credit unions and cooperatives	1 407	1 993	1 632
	<i>Deutsche Bundesbank</i>	14	15	49
	Other	334	328	508
	<b>Total</b>	<b>6 352</b>	<b>7 293</b>	<b>8 143</b>
Insurance companies	Insurance companies	37	39	35
	Insurance agents	-	-	-
	<b>Total</b>	<b>37</b>	<b>39</b>	<b>35</b>
Financial service providers	Financial transfer services	838	1 670	1 779
	Currency services	-	2	2
	Credit cards	82	24	4
	Travelers checks	-	-	-
	Other	-	5	53
	<b>Total</b>	<b>920</b>	<b>1 701</b>	<b>1 838</b>
Investment companies				
	<b>Total</b>	<b>-</b>	<b>2</b>	<b>1</b>
Financing companies	Factoring	-	-	-
	Leasing	3	4	1
	Other	-	4	2
	<b>Total</b>	<b>3</b>	<b>8</b>	<b>3</b>
<b>II. STRs submitted by federal government authorities</b>				
Government authorities	BaFin	1	-	4
	Federal tax authority	261	359	335
	<b>Total</b>	<b>262</b>	<b>359</b>	<b>339</b>
<b>III. STRs submitted with respect to terrorist financing (included in total for item I above)</b>				
	Matches with listed persons	22	28	21
	Criminal association/organization	9	21	10
	Other financing of terrorism	34	53	28
	<b>Total</b>	<b>65</b>	<b>102</b>	<b>59</b>
<b>IV. STRs submitted with respect to "phishing" and "financial agents" (included in total for item I above)</b>				
	"phishing"		121	1 648

		2008	2007	2006
	Use of "financial agents"	971	2 525	265
	Total	971	2 646	1 913

714. For an economy the size of Germany's, with a highly-developed financial services sector which provides near-universal access to such services for its resident population, the level of suspicious transaction reporting appears to be unusually low, even allowing for the fact that one report may contain a batch of individual transactions. It also appears that one reporting institution accounts for approximately 10% of total STRs being filed. In addition, the reporting data are heavily influenced by one particular typology. As indicated in the table, a very substantial number of the STRs (29% of those filed by banks and financial services providers in 2007) concern two related activities: "phishing" and the use of "financial agents" to transfer the proceeds of the primary offense out of the country. Until 2007, the institutions were reporting based on the simple predicate offense of illegally siphoning funds from the victims' account ("phishing"). However, after extensive analysis of the position by the FIU in 2005, the BaFin issued a warning notice to institutions, which subsequently focused on the laundering element, namely, the use of third party accounts to transfer the stolen funds abroad, mostly into Eastern Europe and Russia. Under this structure, the organized gangs persuade third parties (the "financial agents") to lend their accounts to receive the stolen funds (in return for a commission). The funds are then withdrawn in cash by the agent, who subsequently uses the services of licensed money remitters to transfer the proceeds to individuals or accounts outside Germany.

715. If this typology is netted out from the figures, the underlying rate of STR reporting by the financial sector shows a significant decline from 8 107 reports in 2006 to 6 398 in 2007 and 6 341 in 2008. In its 2008 annual report, the FIU attributes the decline to three main factors: the increased complexity of ML techniques; improved security for online banking services; and the increased use of electronic banking systems. The data for the first half of 2009 showed a reversal of the trend, with a 6 percent increase in reports compared with the same period in 2008.

716. Generally, the number of reports being filed appears especially low by comparison with other FATF member countries with a substantial financial sector, as shown by the following table.<sup>62</sup>

Country	2006	2007	2008
Germany	10 020	9 043	7 312
France	12 047	12 481	14 565
Italy	9 601	11 987	14 069
UK	213 561	220 484	210 524
Canada <sup>63</sup>	39 036	50 354	67 740

717. Analytical work by the Fund suggests that most countries assessed LC or higher for Recommendation 13 receive in the range of 15–50 STRs per USD billion of GDP<sup>64</sup>. Countries receiving

<sup>62</sup> Data from FIU annual reports and MERs.

<sup>63</sup> For years beginning April 1.

<sup>64</sup> Fund staff has analyzed STR reporting for 35 countries assessed under the 2004 methodology, including all FATF countries. This work is not yet published. GDP is used to normalize the STR reporting as a proxy variable for the value of the proceeds of crime in need of laundering within a jurisdiction and for the value of transactions in the AML regulated sectors, neither data point being readily available. It is assumed that the criminal economy and the value of transactions conducted in the AML regulated sectors are related to

fewer STRs than this range start to receive criticism for low reporting and those that receive more start receiving criticism for defensive or excessive reporting. Germany's STR reporting rate equates to 2.7 STRs per USD billion of GDP. The Fund has also normalized reporting levels against population<sup>65</sup>. The results suggest that most countries assessed LC or higher for Recommendation 13 receive in the range of 40–200 STRs per 100 000 of population. Germany's STR reporting rate equates to 10.7 STRs per 100 000 of population, and is, therefore, significantly lower than either of the comparative ranges. Fund staff has also analyzed the STR reporting rate for countries with law enforcement type FIUs that are involved in investigating cases of ML and TF. The average number of STRs received by such countries where they have been rated LC or higher is 36.8 STRs per USD billion of GDP and 131.7 STRs per 100 000 of population. Again, both of these averages are significantly above the STR reporting rates for Germany.

718. The assessors acknowledge that some variations in reporting levels between countries can be explained by differences in regime design<sup>66</sup> and by methods used to count STRs (e.g., whether reports relate to individual transactions or to a bundle of transactions associated with the same suspicious activity). However, the level of reporting in Germany is so low, that the assessors find it difficult to conclude that it is adequate, even taking into account these types of differences. As analyzed above, some of the low reporting may be attributable to the identified deficiencies in the reporting obligation, some by the confusion that entities face about their reporting obligations, and some by the practice encouraged by the authorities of only reporting once a prima facie criminal case has been established (also reflected in the declining reporting levels). There is no suggestion that the explanation for the low level of reporting lies in the fact that the financial institutions are failing to take their responsibilities seriously: On the contrary, they appear to devote considerable resources to the process, and there was a general sense, among those institutions to which the assessors spoke, that they were committed to providing quality reports. Rather, the underlying issue appears to be the belief that institutions must undertake extensive investigations of the transactions, the related customer, and the likely predicate offenses before submitting an STR. This view is supported by several factors:

- As mentioned above, the terms in which the legal obligation is drafted indicate that there has to be an element of near-certainty before the report is filed, and this interpretation is widely given to the law by the reporting institutions. Institutions familiar with other reporting regimes considered that the German system required a materially different approach to reporting;
- The reports are filed primarily with the state criminal investigation authorities, and, as a result, they represent criminal complaints which the authorities are obliged to investigate as such in each and every case;
- Institutions and the authorities report that a typical STR might involve quite a substantial dossier of information collected by the institution to establish a level of proof that warrants the criminal complaint. This might typically involve medium or long-term monitoring of accounts to build up the evidence, although it should be noted that such extensive STRs are not encouraged by the AML Act (or by the FIU or the BaFin);

---

the size of the economy, and that, generally, the level of STR reporting should relate to the amount of laundering activity that is taking place—which is some function of the proceeds of crime flowing through the economy.

<sup>65</sup> It is more challenging to justify an assumption that the amount of money laundering activity in an economy is linked to the size of its population. Population, alone does not generally drive economic output—and the criminal economy and money laundering activity are economic outputs.

<sup>66</sup> Differences in regime design that amount to deficiencies against the FATF 40+9 are not legitimate reasons to justify low reporting levels.

- The institutions note that, if they fail to make a substantive case of ML, the STRs may be criticized on the basis that they are of no value to the prosecution services. They report that the expectations of the law enforcement authorities have risen over the years, in that they expect evidence of the actual ML offense, as defined, rather than simply indications that transactions might involve the proceeds of crime; and
- The FIU, in its annual reports, indicates that less than 10 percent of the STRs lead to closure of the case without any residual concern that the reported transaction is linked to criminal activity, and that there is a very high correlation between the suspected predicates reported by the institutions, and the conclusions about the offenses reached by the law enforcement authorities. Moreover, the reporting institutions have been led to believe that the identification of the potential predicate offense is an essential component of the STR.

719. While this process undoubtedly leads to very high quality STRs (and the authorities correctly point to the very high number of investigations that results from the STR submissions relative to other countries), it denies the FIU and the state law enforcement authorities important access to a wider intelligence base (as discussed in section 2 above). In addition, in fulfilling the role of quasi-investigator, there must be doubts as to whether the institutions are effectively complying with the obligation to file reports “immediately” when a suspicion arises, since the construction of the criminal complaint may involve extensive monitoring of transactions over a period of time.

720. With respect to the pattern of reporting across individual parts of the financial sector, it must also be noted that reporting has been almost nonexistent from insurance agents and currency service providers (*i.e.* bureau de change). The latter is particularly surprising (although the number of independent providers, other than the banks, is only 22, and there has been a sharp decline in business since the introduction of the Euro in 2002) and may suggest that an awareness of the issues is lower in these sectors than in others.

721. The analysis of STR filings within each state (below) also show, *prima facie*, some surprising results, particularly in relation to the comparatively low numbers submitted to the authorities in Hesse, which is host to the country’s financial center of Frankfurt. The FIU indicated that it has undertaken extensive analysis of the data, but has been unable to identify any specific patterns or trends that might explain regional variations in the reporting levels. In principle, institutions would be expected to report to the authorities of the state in which the suspicious transaction was identified, but this may not always be the case where institutions have regional or national AML/CFT compliance functions, which may file STRs from a central position, thereby distorting the true source of the underlying report.

<b>STRs filed in individual states</b>			
<b>State</b>	<b>2006</b>	<b>2007</b>	<b>2008</b>
Baden-Württemberg	1 109	934	790
Bavaria	2 164	2 039	1 518
Berlin	573	698	554
Brandenburg	198	234	138
Bremen	131	96	122
Hamburg	420	343	285
Hesse	1 074	930	706
Mecklenburg Western Pomerania	98	104	89
Lower Saxony	747	692	658
North-Rhine Westphalia	2 142	1 760	1 553
Rhineland-Palatinate	339	294	222
Saarland	91	108	64

STRs filed in individual states			
State	2006	2007	2008
Saxony	298	370	178
Saxony-Anhalt	171	132	105
Schleswig-Holstein	336	221	250
Thuringia	160	125	117
Total	10 051	9 080	7 349

### 3.7.2. Recommendations and Comments

722. In considering an appropriate compliance rating for this Recommendation, the assessors have had to balance what are seen to be a range of technical and structural deficiencies against the overall output from the system. There is no doubt that the quality of the STRs is high and that this may contribute to the exceptional levels of ML convictions and orders obtained to forfeit and confiscate assets that are proceeds of crime by international comparison (even though there is no hard evidence to demonstrate this contribution). However, the assessors consider that the “high-quality” STR approach comes at the price of denying the FIU and LEAs a broader intelligence base that would come from a lower evidentiary threshold of reporting. A broader intelligence base may help in efforts to fight more serious ML and also assist efforts to actually confiscate and forfeit more assets that are subject to orders. Thus, denying the FIU and LEAs some intelligence, combined with the technical deficiencies that arise from the legal framework, suggests that the current framework falls materially short of the standard, while still delivering some distinctly positive output.

723. In order to comply fully with Recommendations 13, 14, Special Recommendation IV, and Recommendation 25 (cr. 25.2), Germany should:

#### *With respect to Recommendation 13 and Special Recommendation IV*

- Establish clearly that the legal threshold for STR reporting is an obligation with respect to transactions where the institution suspects or has reasonable grounds to suspect that the transaction involves the proceeds of crime.
- Investigate the reasons for the exceptionally low level of reporting among certain institutions.

#### *With respect to Recommendation 14*

- Extend the tipping-off provision to cover cases where transactions are being reviewed internally to determine whether an STR should be filed.

#### *With respect to Recommendation 25*

- Discuss with the state prosecution authorities the introduction of a common approach to providing feedback to reporting institutions on both the overall quality of reports and their value in terms of investigations and prosecutions.

### 3.7.3. Compliance with Recommendations 13, 14, 19 and 25 (criteria 25.2), and Special Recommendation IV

Rating	Summary of factors underlying rating
--------	--------------------------------------



<b>R.13</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Scope of reporting relates to ML only and not to proceeds of criminal activity.</li> <li>• Threshold for reporting requires a high degree of certainty of an offense, and the report constitutes a criminal complaint.</li> <li>• Reporting obligation does not cover “insider trading and market manipulation,” nor “counterfeiting and piracy of products” as these are not predicate offenses for ML.</li> <li>• Material deficiencies in the TF offense limit the reporting obligation.</li> <li>• High threshold for reporting creates the need for investigation which in turn makes prompt reporting of suspicions impracticable.</li> <li>• Low level of reporting suggests that not all aspects of the regime are working effectively.</li> </ul>
<b>R.14</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Tipping-off prohibition applies only to reports that have already been filed.</li> </ul>
<b>R.19</b>	<b>C</b>	<ul style="list-style-type: none"> <li>• This Recommendation is fully observed.</li> </ul>
<b>R.25</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Very poor specific feedback on STRs filed with the <i>Länder</i> authorities.</li> <li>• Rating for this section: <b>NC</b></li> </ul>
<b>SR.IV</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Threshold for reporting requires a high degree of certainty of an offense, and the report constitutes a criminal complaint.</li> <li>• Material deficiencies in the TF offense limit the reporting obligation.</li> <li>• High threshold for reporting makes prompt reporting of suspicions impracticable.</li> </ul>

### *Internal controls and other measures*

## **3.8. Internal Controls, Compliance, Audit and Foreign Branches (R.15 & 22)**

### **3.8.1 Description and Analysis**

#### ***Legal Framework:***

724. The AML/CFT framework in Germany contains a number of provisions requiring financial institutions to establish internal controls, policies and procedures applicable to the financial sector. The AML Act lays down measures common to all sectors to which the Act applies. In addition, the sector legislation (the Banking Act, the Insurance Supervision Act, and the Investment Act) contain further AML/CFT measures applicable to the various types of financial institutions.

#### ***Establish and Maintain Internal Controls to Prevent ML and TF (c. 15.1, 15.1.1 & 15.1.2):***

725. Section 9 (1) of the AML Act requires credit institutions, financial services institutions, and insurance undertakings to take appropriate internal measures (defined in the legislation as “internal safeguards”) to ensure that they cannot be misused for the purpose of ML and TF. Section 9 (2) requires institutions:

- To designate an ML compliance officer (including at group level) directly subordinate to the management to act as contact for the law enforcement authorities and the BKA (FIU), as well as for competent financial supervisors, and to provide the officer with the means and procedures necessary to carry out his or her responsibilities properly and effectively.

- To develop and update internal policies, appropriate business and customer-related safeguards and controls to prevent ML and TF.

726. Section 9(4) provides that, in individual cases, the competent supervisory authority may give instructions that are appropriate and necessary to implement the internal safeguards as defined in the Act. The authorities are also specifically authorized to permit the internal controls to be applied on a risk-sensitive basis to reflect the type and amount of business conducted by such entities or groups.

727. The foregoing provisions do not apply to insurance intermediaries.

728. The specific legal obligation to appoint a compliance officer, which in substance is unchanged from the previous legislation in place since 1993, is limited in scope, as the legislation defines the role of this person “to act as contact for the law enforcement authorities and by the BKA (FIU) as well as for the BaFin.” The role of the compliance officer is explained in more detail in the Explanatory Memorandum to the AML Act, in the BaFin’s “Guidelines dated December 30, 1997 (but incorrectly dated March 30, 1997 in the English translation) concerning measures to be taken by financial services institutions to combat and prevent ML,” as well as in the BaFin’s public compendium of letters sent to individual financial institutions (*Consbruch*). Similar guidance was provided to credit institutions. There is, however, no explicit legal obligation requiring institutions to ensure that the compliance officer has timely access to CDD information, transaction records, and other relevant information. In the course of regular supervision, the BaFin communicates suggested improvements to individual financial institutions on the basis of the external audit findings (see discussion in Section 3.10 below). Some (notably the larger) financial institutions appear to be allocating a broader mandate to their compliance officers, notwithstanding the explicitly prescribed role as set forth in legislation. Section 25c(2) of the Banking Act and similar provisions in the Investment Act require institutions to operate and update appropriate data processing systems which enable them to recognize business relationships and individual transactions that should be regarded as suspicious or unusual. The BaFin is empowered under this legislation to define criteria for cases in which credit institutions are not required to use automated systems for this purpose. In November 2005, the BaFin specified that financial institutions with income of EUR 250 million (USD 348 million) or less are not required to use such systems. All other credit institutions are subject to the obligation.

729. Section 80d (1) of the Insurance Supervision Act has a very similar provision, except that there is no requirement to implement the monitoring procedures through automated data processing systems.

***Independent Audit of Internal Controls to Prevent ML and TF (c. 15.2):***

730. Section 25a of the Banking Act requires credit institutions and financial services institutions to have a proper business organization which ensures compliance with the legal provisions. This is defined to require appropriate internal control procedures appropriate for the monitoring and controlling of risks, including an internal auditing function (Section 25a(1) sentence no. 3 no. 1 of the Banking Act).

731. Section 64a(1) number 4 in combination with Section 80c(2) of the Insurance Supervision Act impose requirements for all insurance undertakings to have internal auditors and for the internal audit unit to check compliance with requirements to prevent ML and TF at least once a year. The report on audit results must be presented to the management board, the ML compliance officer, and the BaFin.

732. Section 9a of the Investment Act provides that a capital investment company must have an orderly business organization, including appropriate control measures involving the existence of an internal audit function. Section 99(3) of the same Act extends this provision to investment stock corporations.

733. Under the relevant provisions of the German Commercial Code and financial sector legislation, German financial institutions are required to appoint qualified external auditors to perform an annual audit of their financial statements. Refer to section 3.10 for a more detailed discussion of the AML/CFT role played by the external auditors.

***Ongoing Employee Training on AML/CFT Matters (c. 15.3):***

734. Under Section 9(3) of the AML Act institutions are under an obligation to ensure that employees involved in carrying out transactions and for initiating and establishing business relationships are aware of methods of ML and TF and of the requirements of the AML Act.

***Employee Screening Procedures (c. 15.4):***

735. There are no explicit provisions in the AML Act or in other legislation which oblige financial institutions to ensure high standards when hiring employees. As noted above, the AML Act obliges financial institutions to develop and update internal principles, appropriate business and customer-related safeguards and controls to prevent ML and TF. The Explanatory Memorandum to the AML Act states that the word “controls” means: “Controls as referred to in No. 2 refer to the internal principles and safeguards, including monitoring systems, of the company and to the reliability of company employees, where they deal with carrying out transactions or at least to participate in them, such as mediators or external service providers.” The German authorities advised the assessors that when checking employee reliability, financial institutions may exercise a great deal of discretion with regard to the frequency of checks and the instruments used. It is also up to the company to decide the process for performing checks on existing employees. Regular checks of employee reliability during employment are needed only in exceptional, justified cases.

***Additional Element – Independence of Compliance Officer (c. 15.5):***

736. The Explanatory Memorandum to the AML Act clearly indicates that it is intended that the compliance officer is to be independent of management.

***Application of AML/CFT Measures to Foreign Branches & Subsidiaries (c. 22.1, 22.1.1 & 22.1.2 and additional element 22.3):***

737. In this section, a “third state” is a country other than an EU or EEA member state.

738. Under Section 9(2) of the AML Act financial institutions must ensure that all subsidiaries and branches appoint ML compliance officers. In addition, under Section 25g of the Banking Act, financial institutions which are subject to the Banking Act must:

- Create group-wide internal safeguards under Section 25c(1) of the Banking Act (discussed under Recommendation 15, above);
- Ensure compliance with the due diligence requirements of Sections 3, 5 and 6 of the Money Laundering Act and Sections 25d and 25f of the Banking Act; and
- Ensure compliance with the record-keeping requirements of Section 8 of the AML Act.

739. Financial holding companies and mixed holding companies as defined under the Banking Act are explicitly subject to the AML Act and are supervised by the BaFin.

740. If the required measures are impermissible or “not actually practical” under the law in a “third state” (i.e. non-EU or EEA countries) in which the subsidiary or branch is resident the parent financial institution must ensure that the subsidiary or branch in such state does not establish or continue business relationships and does not undertake transactions (third sentence of Section 25(g) of the Banking Act, which is also applicable to investment companies). For an existing business relationship, the parent financial institution must ensure that such relationship is terminated by giving notice of termination or by other means regardless of other legal or contractual provisions.

741. In the event that stricter requirements apply at the registered office abroad of a subsidiary or a branch, such stricter requirements shall be met there.

742. The prohibition to establish or continue a business relationship and the duty to ensure that a relationship is terminated in Section 25g of the Banking Act entered into force on March 25, 2009, less than two months prior to the on-site visit. Therefore, it was not possible to determine if any situations had arisen in practice where German financial institutions had encountered situations in other countries where the prescribed measures were “not practical.”

743. Section 80d(3) of the Insurance Supervisory Act requires insurance undertakings which are parent companies of a group or conglomerate to

- Create internal safeguards under Section 9 of the AML Act applicable to their branches and subsidiaries;
- Ensure compliance with Sections 3, 5 and 6 of the AML Act by their branches and subsidiaries; and
- Ensure compliance with Section 80e (simplified due diligence requirements) of the Insurance Supervisory Act.

744. These measures must be taken when permitted by the legislation of the country in which the subsidiary or branch is located.

745. If stricter measures apply in the third country in which an insurance undertaking or subsidiary is located, those stricter requirements shall be met in that country.

746. There are no provisions explicitly or otherwise requiring financial institutions to pay particular attention to the principle of equivalency to German standards in respect of subsidiary or branch operations in EU or EEA member states that do not, or insufficiently, apply the FATF Recommendations.

***Requirement to Inform Home Country Supervisor if Foreign Branches & Subsidiaries are Unable to Implement AML/CFT Measures (c. 22.2):***

747. Section 80d(3) of the Insurance Supervisory Act provides that in cases where the legislation of the third country where the insurance undertaking is located does not permit application of the above measures, the insurance undertaking or its parent shall immediately inform its supervisory authority (in almost all cases, the BaFin) and take additional measures to effectively handle an enhanced risk of ML or TF.

748. In its previous version, Section 25g of the Banking Act required financial institutions to notify the BaFin if foreign branches and subsidiaries of banks or investment firms were unable to implement AML/CFT measures. In its current wording, in force since March 25, 2009, it goes further by explicitly

prohibiting financial institutions from establishing or continuing business relationships and operations in countries (other than EU or EEA member states) under these circumstances.

### ***Effectiveness of Implementation***

749. The German legal obligations in place implementing internal controls, including compliance management and internal audit, are in some places narrowly focused, and there are gaps in the application of group-wide standards as noted below. For example, although there is no legal obligation to ensure that compliance officers have timely access to CDD information, it is clear that the compliance officers are intended to be independent from management in carrying out their duties. The move towards a risk-based approach to AML/CFT procedures will present a challenge to many financial institutions, which historically have been used to operating in a rules-based regulatory system. Some institutions, especially smaller institutions, are clearly looking to the BaFin to provide greater guidance on what is actually expected, and there seems to be a certain degree of concern that there will be a difference of interpretation between the regulators and individual institutions over what constitutes an adequate set of internal controls and procedures. This will require careful monitoring and engagement by the BaFin, particularly in the development of the private sector guidance discussed in more detail above. As noted in Section 3.10, the BaFin will begin receiving audit reports on the first full year of implementation of the risk-based measures in 2010. It is, therefore, too early to assess the effectiveness of the internal controls and cross-border measures as they apply to such measures.

750. The legal obligation to provide employee training is specifically directed at those employees “involved in carrying out transactions” and for “initiating and establishing business relationships.” However, the requirements do not explicitly require that employees be kept informed of new developments including information on current ML and TF techniques, methods and trends, nor do they require that there is a clear explanation of all aspects of AML/CFT and suspicious transaction reporting.

751. The assessors’ impression from meetings with the private sector was that the larger financial institutions are probably applying a broader interpretation of the legal requirements, but that smaller firms generally tended to take a narrower approach more consistent with the legislated standards. Due to the large size of the financial sector, the numbers of regulated financial institutions, and the wide range of size of institutions, it was not possible to arrive at an overall view of how the financial sector as a whole implements the internal control requirements.

752. The derogations applicable to branches and subsidiaries located in EEA or EU member states with respect to the implementation of group-wide standards (Rec. 22) are significant. The authorities advised the assessors that, at the time of the on-site visit, there were 331 branches of subsidiaries of German financial institutions outside Germany. Of these, 226 (nearly 70%) were located in EEA or EU member states. Finally, the Banking Act measures with respect to branches and subsidiaries outside Germany only came into effect shortly before the on-site visit and therefore it was too early to assess their effectiveness.

### ***3.8.2. Recommendations and Comments***

753. In order to comply fully with Recommendations 15 and 22, Germany should:

#### ***With respect to Recommendation 15:***

- Ensure that the compliance officer is required to have timely access to relevant CDD information.

- Introduce enforceable measures requiring financial entities to provide AML/CFT training to all staff; to require that employees be kept informed of new developments including information on current ML and TF techniques, methods and trends; and to require that there is a clear explanation of all aspects of AML/CFT and suspicious transaction reporting.
- Introduce enforceable measures requiring financial institutions to apply screening procedures at the time of hiring all staff.

***With respect to Recommendation 22:***

- Introduce enforceable measures requiring all financial institutions to pay particular attention to branches and subsidiaries in countries that do not, or insufficiently, apply the FATF Recommendations.
- Ensure that the provisions of section 25g of the Banking Act apply to subsidiaries and branches located in EEA and EU states.
- Ensure that uniform standards are applied in the three principal sectors (banking, insurance and investment firms).
- Implement an enforceable obligation for banks and investment firms to inform German supervisory authorities immediately when a foreign branch or subsidiary (including those in EEA states) is unable to observe appropriate AML/CFT measures.

**3.8.3. Compliance with Recommendations 15 & 22**

	Rating	Summary of factors underlying rating
R.15	PC	<ul style="list-style-type: none"> <li>• The compliance officer measures do not apply to the insurance intermediaries sector.</li> <li>• No legal obligation to ensure that the compliance officer has timely access to relevant CDD information.</li> <li>• No obligation to provide training to staff other than those involved in dealing with customers or carrying out transactions.</li> <li>• No legal obligations imposed on financial institutions requiring them to put in place screening procedures to ensure high standards when hiring employees.</li> <li>• Application of measures across corporate groups is new and effectiveness could not be assessed.</li> </ul>
R.22	LC	<p>Scope limitations:</p> <ul style="list-style-type: none"> <li>• No measures which explicitly require financial institutions to pay particular attention to their branches and subsidiaries in EU or EEA member states that do not, or insufficiently, apply the FATF Recommendations.</li> <li>• Obligation to notify authorities of inability to implement AML/CFT measures does not apply to EU or EEA financial institutions other than insurance undertakings.</li> </ul>



### 3.9. Shell Banks (R.18)

#### 3.9.1. Description and Analysis

##### *Prohibition of Establishment Shell Banks (c. 18.1)*

754. The BaFin does not permit the establishment of shell banks within Germany. While there is no statutory prohibition on such entities, the possibility of creating a shell operation is precluded through the licensing and supervisory processes, which require that licensed institutions have, among other things, an appropriate organizational and management structure. For example, Section 33(1) of the Banking Act provides that one of the grounds for refusing authorization may lie in the fact that the applicant has not made appropriate organizational arrangements. There is no evidence to suggest that the BaFin's licensing regime has failed to prevent the creation of shell banks within the jurisdiction.

##### *Prohibition of Correspondent Banking with Shell Banks (c. 18.2)*

755. Initiating and continuing a correspondent or other business relationship with a shell bank, as defined in Article 3(10) of the Third EC Money Laundering Directive, are explicitly prohibited under Section 25h of the Banking Act. In this context, 'shell bank' means a credit institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence, or meaningful mind and management, and which is unaffiliated with a regulated financial group.

##### *Requirement to Satisfy Respondent Financial Institutions Prohibition of Use of Accounts by Shell Banks (c. 18.3)*

756. According to Section 25f (2) of the Banking Act, credit institutions must take measures to ensure that any respondent institution does not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank. This also includes the prohibition for the credit institution to establish or maintain a correspondent banking relationship with a respondent institution that is known to permit its own accounts to be used by a shell bank. However, these obligations only apply with respect to relationships with financial institutions outside the EU on the basis that all EU institutions are prohibited under the Third EC Money Laundering Directive from providing such facilities to shell banks.

757. Through its administrative arrangements, the BaFin requires that institutions obtain a contractual declaration from non-EU credit institutions wishing to establish or maintain a correspondent banking relationship, stating that the foreign credit institution is not a shell bank, does not permit its own accounts to be used by a shell bank and has no other business relationships with shell banks.

#### 3.9.2. Recommendations and Comments

None

#### 3.9.3. Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18	C	This Recommendation is fully observed.

**Regulation, supervision, guidance, monitoring and sanctions****3.10. The Supervisory and Oversight System – Competent Authorities and SROs. Role, Functions, Duties, and Powers (Including Sanctions) (R. 23, 29, 17 & 25)****3.10.1 Description and Analysis**

***Competent authorities – powers and resources: Designation of Competent Authority (c. 23.2); Power for Supervisors to Monitor AML/CFT Requirement (c. 29.1); Authority to conduct AML/CFT Inspections by Supervisors (c. 29.2); Power for Supervisors to Compel Production of Records (c. 29.3 & 29.3.1); Adequacy of Resources – Supervisory Authorities (R.30)***

758. Section 16 (1) of the AML Act designates the competent authorities responsible for enforcing the provisions of the Act. It provides that such authorities “may take the appropriate and necessary measures and orders to ensure compliance with the requirements of this Act. To do so, they may exercise the authority granted to them for other supervisory tasks”.

759. The BaFin is the federal prudential supervisor for virtually all financial institutions in Germany, and as such, Section 16(2) gives it AML/CFT supervisory responsibility for all credit institutions (apart from the Development Loan Corporation – KfW), financial services institutions, domestic branches of credit institutions and financial services institutions with head offices abroad, investment companies and investment management companies.

760. The BaFin is also the designated authority for all private-sector insurance companies and all public-sector insurance companies that operate in more than one *Land* within Germany. Public-sector insurance companies that operate in one *Land* only are subject to supervision by the local *Land* authorities. At the time of the on-site visit, there were only three public-sector insurance companies in Germany that fell into this category: two in Lower Saxony and one in Saxony-Anhalt. The competent authorities in these *Länder* are the Ministry of Economic Affairs, Labor and Transport and the Ministry of Economics and Labor, respectively. The three public-sector companies are relatively small and as such only form a tiny part of the German insurance sector.

761. Insurance intermediaries which operate throughout Germany, also fall to the *Länder* authorities to supervise for AML/CFT purposes, although it is unclear exactly which ministry or department in each *Land* fulfils the role. *Länder* AML/CFT supervisory responsibilities for insurance intermediaries are typically housed in “Regional Commissions.” These municipally-based bodies are responsible for functions that are not specifically assigned to a particular *Land* agency. In Hesse there are three such bodies, and the assessors met with officials of the Wiesbaden Regional Commission. Most of their responsibility revolves around agent licensing, and their role in AML/CFT supervision is not clear.

762. The Federal Ministry of Finance (MoF) is responsible for the AML/CFT supervision of the KfW, which is subject to the AML Act. MoF officials confirmed there is no active supervision by the MoF of the KfW. However, the KfW has transferred most of its active lending into a new banking subsidiary, which is a credit institution as defined under the Banking Act. As such, this subsidiary is supervised by the BaFin. The German Central Bank (*Bundesbank*) is also subject to the AML Act, but is not supervised. It only holds accounts for its employees.

763. Section 16(1) of the AML Act provides that sector regulators may take the appropriate and necessary measures and orders to ensure compliance with the requirements of the AML Act, and that in doing so, they may exercise the authority granted them for other supervisory tasks. The authority granted the BaFin for other supervisory tasks is contained in its mandate under the Federal Financial Supervisory Authority Act, and the relevant provisions of the sector legislation (the Banking Act, the Insurance

Supervision Act, and the Investment Act). The BaFin and the *Länder* authorities are specifically empowered to apply specific administrative fines set out in the AML Act.

764. The sector laws have provisions which, in general, give the BaFin a broad range of traditional prudential regulatory tools. For example, Section 44(1) of the Banking Act obliges credit and financial institutions to provide, upon request, information on all business activities and to submit documentation to the BaFin, to any persons whom the BaFin may use to conduct examinations, and to the *Bundesbank* (however, the *Bundesbank* has not been delegated to perform audits on AML/CFT). The BaFin is authorized to perform audits at institutions with or without cause, and this power may be delegated to the *Bundesbank*. The BaFin, and its employees and agents, may enter the business premises of financial institutions for these purposes during customary business hours. The *Länder* authorities have the same powers as the BaFin with respect to those insurance undertakings that they supervise. Under Section 44(6) of the Banking Act, a person required to provide information to the BaFin may only refuse to answer questions if the replies given would expose that person or a related person to the risk of criminal prosecution under the Banking Act or the Administrative Offenses Act.

765. Under Section 7 of the Banking Act, the BaFin is required to cooperate with the *Bundesbank* in respect of the ongoing monitoring of institutions. The *Bundesbank*'s role essentially comprises assessing the adequacy of institutions' capital and risk management procedures, and appraising audit findings. The BaFin is required, in general, to base its prudential supervisory measures on the auditing findings and appraisals made by the *Bundesbank*. The BaFin and the *Bundesbank* are authorized to share information with each other for these purposes. Although the *Bundesbank* plays a key role in the overall supervision of the financial sector and works closely with the BaFin in doing so, it has no day-to-day role in the supervision of AML/CFT compliance by institutions. Prudential guidelines issued to financial institutions by the BaFin must be agreed by the *Bundesbank*; however, this does not apply to AML/CFT guidance issued by the BaFin.

766. The BaFin is a federal public agency subject to the oversight of the Federal Ministry of Finance, but is otherwise operationally independent in the exercise of its functions (Section 2 of the Financial Services Supervisory Authority Act), and has control over its revenue and expenses. The BaFin's budget is prepared separately from the Federal Government budget. The total budget for 2008 amounted to EUR 120.4 million (USD 168 million), and for 2009, it is anticipated to be EUR 135.3 million (USD 188 million). The increase is attributed principally to increases in staff count and salaries. According to Sections 13–16 of the Financial Services Supervisory Authority Act, the BaFin covers its expenses by means of its own revenues obtained from fees, cost recovery, and cost allocation to the supervised financial sector. This ensures that the BaFin is financially independent from government and has the necessary budgetary means to supervise the financial sector, including access to all the administrative and technical resources, databases, IT processing and other tools that are necessary for it to meet its mandate.

767. Independence from the supervised financial sector and standards of professional behavior are enforced through a code of conduct applicable to the BaFin senior management as well as an anti-corruption program for the entire staff. Recruitment procedures include selection, written and oral presentations, an assessment center, and a language test (English). Successful candidates must have graduated with certain minimum grades, and have the necessary skills and personal integrity. Criminal background checks are run on applicants by inspecting their police clearance certificates; applicants who have an entry in their police clearance certificate are not accepted.

768. A high standard of confidentiality is ensured by legal provisions as well as contractual confidentiality obligations. The most specific legal provisions relating especially to the BaFin are contained in Section 9 of the Banking Act, Section 84 of the Insurance Supervision Act, and Section 5b of the Investment Act. According to these provisions, employees of the BaFin may not disclose or use

without authorization facts (especially business and trade secrets) that have come to their attention in the course of their activities and which should be kept secret in the interests of the institution or a third party. This requirement continues to apply after they have left such employment or their activities have ended. Each employee of the BaFin must sign an individual confidentiality agreement, in addition to the employment contract when starting work with the BaFin.

769. All of the BaFin's responsibilities in connection with AML/CFT and financial fraud have been grouped together within the BaFin since the beginning of 2003 in the Money Laundering Prevention Group (MLPG), which is a part of the BaFin's Corporate Services Directorate. The BaFin's Prudential Supervisory Directorate (which has a staff complement of 841) is responsible for applying market entry requirements in all sectors (except for money remitters, currency dealers and credit card businesses), and for ongoing prudential supervision. Although the MLPG deals directly with supervised entities on AML/CFT matters, it regularly liaises with the prudential supervisors on common areas of supervision such as the quality of risk management and controls.

770. The MLPG has about 90 staff and consists of the following six sections:

- **Section GW 1** (10 staff) is responsible for legal, international and policy matters and the interpretation of all AML/CFT provisions;
- **Section GW 2** (14 staff) monitors the AML/CFT obligations under the AML Act and the Banking Act applicable to all credit institutions (2 048 entities) and 4 credit card businesses. With regard to the latter, GW 2 is also responsible for regular supervisory duties in accordance with the Banking Act. However, the amount of time spent on such supervisory work is nominal compared to AML/CFT supervision;
- **Section GW 3** (18.5 staff) monitors the implementation of the AML/CFT obligations arising from the AML Act and the Banking Act in respect of all financial services institutions and insurance undertakings (156 insurance companies and 720 financial services institutions not including financial leasing and factoring firms. In addition, the section also exercises supervisory duties under the Banking Act with regard to 39 money transmission businesses and 18 currency exchange businesses. GW 3 is also responsible for prosecuting unlicensed money transmission service, currency exchange and credit card businesses;
- **Section GW 4** (33 staff) is responsible for the management of an automated account access system established on April 1, 2003 in accordance with Section 24c of the Banking Act, and for applying special measures according to Section 6a of the Banking Act (see section 7.2 below for more information about this system);
- **Section GW 5** (8 staff) carries out prudential as well as AML/CFT supervision of 318 financial leasing and factoring firms located in the southern regions of Germany;
- **Section GW 6** (7 staff) carries out prudential as well as AML/CFT supervision of 245 financial leasing and factoring firms located in the northern regions of Germany.

771. The BaFin's general training program for all employees includes a special module on AML/CFT. New employees starting in the MLPG participate in a training program designed especially for this Group and are introduced into practical work by their colleagues. Within the MLPG, the respective divisions present training on new developments in the field of AML/CFT (for example, the new AML Act). Apart from that, representatives of the MLPG take part in international training programs, either as speakers or members of the audience, and also regularly attend international working groups and conferences, thus

enabling them to stay up to date with international developments. Overall, the MLPG appeared to be well resourced by high-quality staff, all specialists in the field of AML/CFT.

772. With respect to supervision of the insurance sector that does not fall under the BaFin, the information available to assessors indicated that an appropriate level of resources appears to be assigned to AML/CFT supervision of the three public sector insurance companies supervised by Saxony Anhalt and Lower Saxony. Generally speaking, the BaFin's procedures and processes seem to be followed. As regards the supervision of insurance intermediaries and financial enterprises, a detailed assessment was not made, but the facts available indicated that the *Länder* authorities (Regional Commissions) assign a low level of priority to ensuring that insurance intermediaries (approx. 72 000) comply with the AML Act. Supervision of insurance intermediaries is a part time job for those responsible.

***Sanctions: Powers of Enforcement & Sanction (c. 29.4); Availability of Effective, Proportionate & Dissuasive Sanctions (c. 17.1); Designation of Authority to Impose Sanctions (c. 17.2); Ability to Sanction Directors & Senior Management of Financial Institutions (c. 17.3): Range of Sanctions – Scope and Proportionality (c. 17.4)***

773. The BaFin is the designated competent AML/CFT supervisory authority with the powers to apply sanctions for noncompliance with the AML Act and sector- specific laws (Banking Act, etc).

774. The statutory sanctions available vary according to the laws on which they are based. The AML Act specifically provides for a number of administrative fines for failure to comply with preventive measures set out in the AML Act. Failure to comply with AML/CFT measures that are contained in sector-specific legislation, such as the Banking Act, may be sanctioned on the basis of the powers granted to the BaFin under such laws.

#### *Administrative Fines*

775. Under the AML Act, the BaFin may apply certain administrative fines set out in the AML Act to specified violations of that Act (more detail below). These administrative fines apply to all sectors under the BaFin's purview. There are also certain administrative fines set forth in the Banking Act, the Insurance Supervision Act, and the Investment Act for violations of these Acts: these are discussed further below.

776. Although administrative fines can be imposed by the BaFin or other administrative authorities, for procedural purposes they are considered to be part of criminal law. They are governed by the Administrative Offenses Act, which follows the structure of the CC. Pursuant to Section 46 (1) of the Administrative Offenses Act, the CPC applies where the Administrative Offenses Act does not rule otherwise. This means that administrative fines are subject to the fundamental principle of certainty in criminal law ("*strafrechtliches Bestimmtheitsgebot*"), which is anchored in Article 103(2) of the Basic Law. The German authorities have confirmed that, under this principle, criminal provisions (including those regarding administrative offenses) must be sufficiently precise and defined by law that their scope and consequences are clear and understandable. Therefore, there is no "blanket clause" for administrative offenses; instead, all elements of an offense must be clearly specified. For example, an administrative fine for failure to comply with Section 9(1) of the AML Act ("take appropriate internal measures") would not conform to this fundamental principle because the obligation is not sufficiently precise and defined to qualify for criminal prosecution. This would apply notwithstanding any guidance issued by the BaFin; the German authorities confirmed to the assessors that the BaFin's guidance does not have the status of law and, hence, cannot amend or specify the elements of an offense in criminal law. Overall, this fundamental principle results in a limited catalogue of AML/CFT administrative offenses, as indicated below.

777. Section 17 (1) of the AML Act states that anyone who intentionally or by gross negligence commits one of the following will be liable for a fine of up to EUR 100 000 (USD 139 170):

- Failure to identify a contracting party.
- Failure to record information correctly or completely.
- Failure to keep records and other evidence of business relationships and transactions. Or
- Failure to report suspicious activity.

778. Section 17(2) states that anyone who commits one of the following intentionally (viz., excluding gross negligence) will be liable for a fine of up to EUR 50 000 (USD 69 585).

- Failure to clarify whether the contracting party is acting on behalf of a beneficial owner;
- Failure to find out the name of the beneficial owner;
- Failure to verify the identity of a contracting party or to ensure that the first transaction is carried out through an account opened in the contracting party's name; or
- Disclosure of information relating to an STR to the customer concerned or to institutions or persons other than those permitted.

779. The BaFin may also apply administrative fines under the sector-specific laws. For example, Section 56 of the Banking Act provides for a number of sector-specific offenses for which the BaFin may apply an administrative fine up to the maximum specified, as follows:

- Failure to comply with an enforceable order to dismiss a manager etc., a maximum fine of EUR 500 000 (USD 695 850);
- Failure to maintain a data file for the automated account access system, or not doing so correctly or completely; or failure to ensure that the BaFin has access at all times to the financial institution's data files through the automated account access system: a maximum fine of EUR 150 000 (USD 208 755);
- Establishment or continuation of a correspondent or other business relationship with a shell bank: a maximum fine of EUR 150 000 (pursuant to Section 143(3) no. 1 of the Investment Act this fine is also applicable to investment companies);
- Establishment or continuation of a payable-through account; a maximum fine of EUR 150 000 (USD 208 755); and
- Intentional or negligent failure to comply with Regulation 1781/2006 on wire transfers, for which there is also a list of more specific offenses relating to the individual obligations under that Regulation: a maximum fine of EUR 50 000 (USD 69 585).

780. Section 144 of the Insurance Supervision Act allows the BaFin and the *Länder* authorities to apply administrative fines for failure to comply with an enforceable order to dismiss a manager, etc., for which the maximum fine is EUR 150 000 (USD 208 755). Similar provisions in the Investment Act apply,



for which the maximum fine is EUR 100 000 (USD 139 170). In addition, this Act also enables the BaFin to apply administrative fines for failure to maintain a data file for the automated account access system, or not doing so correctly or completely, or failure to ensure that the BaFin has access at all times to the investment firm's data files through the automated account access system: to a maximum fine of EUR 150 000 (USD 208 755).

781. The only sector-specific AML obligation in the Insurance Supervisory Act and the Investment Act, is an obligation to implement appropriate internal safeguards. However, non-compliance with these obligations does not attract an administrative fine (similar to the situation under the Banking Act). The authorities advised the assessment team that the reason for this is that the internal safeguard obligations are not sufficiently precise and defined to qualify for the application of administrative fines under the principle of certainty (described above). Because of this, the Insurance Supervisory Act and the Investment Act do not grant additional powers to apply AML-specific administrative fines (except for Section 143(3) no. 1 of the Investment Act.

782. Although as a general principle, there is no criminal liability for legal persons under German law, both natural and legal persons are subject to administrative fines for failure to comply with AML/CFT requirements (regardless of whether these are contained in the AML Act or in sector legislation). The liability of legal and natural persons is regulated by Sections 30 and 130 of the Administrative Offenses Act. Section 30 of the Administrative Offenses Act addresses situations involving breaches of law by legal persons or associations of persons, and provides that where someone acting in a prescribed capacity has committed a criminal offense or a regulatory offense which results in a legal person or association of persons violating a provision, a regulatory fine may be imposed on such legal person. The prescribed capacities which trigger this provision are individuals acting:

- a. As an entity authorized to represent a legal person or as a member of such an entity;
- b. As Chairman of the executive committee of an association without legal capacity or as a member of such a committee;
- c. As a partner authorized to represent a partnership with legal capacity;
- d. As the authorized representative with full power of attorney or in a managerial position as procura-holder or a commercial power of attorney of a legal person or association of legal persons; or
- e. As another person responsible on behalf of the management of the operation or enterprise forming part of a legal person, or an association of legal persons referred to in items 2 and 3 in the foregoing, also covering supervision of the conduct of business or other exercise of controlling powers in a managerial position. Although members of the supervisory board are not explicitly mentioned in the text of the Act, they are in fact covered (as confirmed by the explanatory memorandum for the amendments to the Act). While Section 405(1) of the Stock Corporation Act does provide for administrative fines (some of which are also applicable to members of the supervisory board), these do not include failure to supervise the management. Such failure may only result in civil liability against the legal person if the failure results in damages (section 116 in conjunction with section 93(2) of the Stock Corporation Act).

783. Section 130 of the Administrative Offenses Act stipulates that any neglect of duty to supervise on the part of the owner of a company (including an entity representing the legal owner, a partner authorized to represent a commercial partnership, or a statutory representative of the owner) which enabled a criminal offense (or administrative or regulatory offense) to be committed, or which merely considerably facilitated

the commission, will constitute an administrative/regulatory offense. This, in turn, can form the basis for the liability of a legal person pursuant to Section 30 of the Act, so that offenses committed by employees who themselves are not in a leading position can be assigned to the legal person. Section 130 does not apply to members of supervisory boards as they are not responsible for the supervision of staff other than management staff.

#### *Administrative Payments (Zwangsgeld)*

784. Under Section 17 of the Financial Services Supervisory Act, the BaFin may impose administrative payments to a maximum of EUR 250 000 (USD 347 925). Administrative payments are a supervisory tool applied in individual cases by the BaFin for failure to comply with supervisory directions. They are not administrative fines and are designed as an incentive to good behavior as opposed to a punishment for bad behavior (viz., violations of law for which specific administrative fines are set out in legislation). There is no limit on the number of repeated administrative payments which may be applied to the same failure.

785. The BaFin's MLPG uses the threat of administrative payments about 20 times each year, mainly to enforce supervisory orders, including formal administrative requests to provide information and documents. While most supervised institutions usually comply with such requests without a formal order, on rare occasions it is necessary to issue formal orders against a supervised institution in order to reach compliance. For example, in 2007, Section GW 3 ordered a major money remittance company to apply enhanced identification requirements in suspected cases of "financial agents/financial mules." It has to be emphasized, however, that this order enforced a prudential course of action as opposed to a violation of the AML Act.

#### *Supervisory Measures*

786. The BaFin issues "serious warning" letters in situations where no specific administrative fine would apply, or where a financial institution would be approaching the criteria laid out in the Banking Act for the BaFin to dismiss a manager. In these letters the BaFin typically requires that identified risk management deficiencies be remedied immediately, under threat of an order under the applicable governing legislation (which, if not complied with, can be enforced with an administrative payment, not an administrative fine—see above). In practice, the BaFin escalates its contact with the financial institution to a meeting at the BaFin's offices where the issues are discussed.

787. However, the BaFin may only order the revocation of licenses, dismissal of managers, or both, under the sector-specific laws, and more particularly in the circumstances set out in Sections 35 and 36 of the Banking Act, and Section 87 of the Insurance Supervision Act and Sections 17a, 97(3), and 17(2) of the Investment Act. These address, *inter alia*, licensing and prudential procedures, which include in particular "reliability" (*Zuverlässigkeit*) of managers. This entails that if a manager is no longer "reliable," the manager may be dismissed by the BaFin on these legal grounds.<sup>67</sup> "Reliability" is no longer given in case of any violations of business related laws (which includes the AML Act for financial institutions). Furthermore, in the case of the Banking Act (Section 36) "intentional or reckless" contravention of, *inter alia*, the AML Act, is explicitly mentioned as a reason for the dismissal of managers. Similar considerations apply with respect to the power to revoke the license. The assessors were unable to test the

<sup>67</sup> For the Banking Act: Section 36(1) sentence 1 in connection with Section 35(2) No. 3 in connection with Section 33(1) No. 2 in connection with Section 1(2) sentence 1; for the Insurance Supervisory Act: Section 87(6) No. 1 in connection with Section 8(1) sentence 1 No. 1 in connection with Section 7a(1); for the Investment Act: Section 17a(1) (capital investment companies) or Section 97(3) (investment stock corporations), each in connection with Section 17(2) sentence 1 No. 3 in connection with Section 7b No. 3.

effectiveness of these provisions given the restriction and also the absence of dismissals and license revocations for AML/CFT reasons.

788. Under Section 81 of the Insurance Supervision Act, the BaFin may issue any orders with respect to insurance undertakings, the members of their management boards and other managers, or persons controlling the undertakings, which are appropriate and necessary to prevent or remedy irregularities. An irregularity is defined as conduct conflicting with the framework of general legal supervision and specific financial supervision; and ensuring that the interests of the insured are adequately safeguarded (safety and soundness requirements). Section 87 of the Insurance Supervision Act provides the legal basis for the BaFin to issue written warnings, to dismiss managers, or to withdraw licenses, in the following circumstances:

1. The insurance undertaking no longer satisfies the requirements for authorization;
2. The insurance undertaking seriously breaches its obligations under the law or the operating plan; and
3. There is evidence of irregularities so serious that continuation of business will jeopardize the interests of the insured.

789. As can be seen, these causes of action do not include AML/CFT violations.

790. In cases where the failure to comply with the required provisions is not a specified offense, the authorities must rely upon their ability to issue supervisory instructions to the institution to address the deficiency. Failure to respond appropriately to the instruction can result in an administrative payment, which can be increased for repeated failures. As noted above, however, the administrative payment is incurred for failure to respond to the instruction, rather than for the original deficiency.

791. Since 2003, the BaFin has revoked the licenses of five financial services institutions (money remitters and bureaux de change) for violations of reporting and other AML/CFT obligations.

792. There are no additional civil sanctions in Germany for failure to comply with national AML/CFT requirements.

793. The following table sets out the numbers of written warnings on AML/CFT issued to financial institutions by the BaFin:

Year	2004	2005	2006	2007	2008	2009 (9 March 09)
Written Warnings	3	12	10	16	14	9

794. In terms of the application of sanctions, since 2001 the BaFin has applied one (1) administrative fine for an AML/CFT failure (under the authority of the predecessor legislation to the AML Act), but has never applied any fines or dismissed any managers for AML/CFT failures under the authority of the sector-specific regulatory laws (although on two occasions the BaFin threatened dismissal action). Five money service remitters' licenses were revoked for AML/CFT reasons. No other sanctions have been applied beyond written warnings. Equally, there have been no other sanctions for failures to comply with AML/CFT obligations. The same appears to be the case with respect to the *Länder* authorities which oversee the insurance companies not subject to the BaFin's supervision, and the insurance intermediaries and financial enterprises.

***Market entry: Fit and Proper Criteria and Prevention of Criminals from Controlling Institutions (c. 23.3 & 23.3.1); Licensing or Registration of Value Transfer/Exchange Services (c. 23.5); Licensing of other Financial Institutions (c. 23.7):***

795. The competent supervisors in each sector are responsible for enforcing market entry requirements (essentially, the BaFin for most of the financial sector, and *Länder* authorities in respect of insurance undertakings supervised by authorities in those *Länder*.) In the following discussion, reference is made throughout to the powers granted to the BaFin, but from a procedural point of view, the two *Länder* that supervise the three public-sector insurance undertakings noted above follow administrative procedures which essentially mirror those of the BaFin. There are, however, special provisions for branches of institutions established in other EU member states (see below).

796. Similar market entry criteria are established for credit institutions, financial services institutions, insurance undertakings, capital investment companies and investment stock corporations according to the Banking Act, the Insurance Supervisory Act, and the Investment Act, respectively. Money remittance, foreign currency dealing, and credit card businesses, if organized on a commercial basis, are defined as financial services institutions under the Banking Act. Therefore, all the measures for licensing, as provided by the Banking Act, apply to such entities.

797. The German Parliament has enacted a new Payment Services Supervisory Act which is anticipated to enter into force in November 2009. At that time, money remittance businesses will no longer be defined as financial services institutions under the Banking Act, but as payment institutions under the Payment Services Supervisory Act. However, the Payment Services Supervisory Act will contain identical provisions on market entry as the Banking Act. Payment institutions will remain under the supervision of the BaFin.

798. A qualified participating interest is deemed to exist if at least 10 percent of the capital of, or the voting rights in, an enterprise is held directly or indirectly through one or more subsidiaries or a similar relationship, or through collaboration with other persons or enterprises, in the holder's own interest or in the interest of a third party; or if a significant influence can be exercised on the management of another enterprise. This definition of "holding" includes not only the immediate holder but also the beneficial owner of such interests. If any holder of a qualified participating interest subsequently intends to increase the amount of the interest over certain thresholds (20%, 33%, or 50% of the voting rights or of the capital), they must notify the BaFin about their intentions without delay.

799. An institution with qualified participating interests applying for a license must submit all relevant data (names of holders, amount of participating interests, professional qualifications and trustworthiness of holders or of the legal representatives or of the general partners). For credit institutions, financial services institutions, and insurance undertakings, if holders belong to a group, details of the structure of the group and their annual audited accounts for the last three financial years must be supplied. Holders must also submit a declaration on:

- Their criminal record, with information on any pending or previous criminal proceedings, including ones related to administrative fines concerning business activities, as well as any sentence or another sanction applied;
- Involvement as a debtor in insolvency proceedings or proceedings regarding the provision of a sworn statement of assets or comparable proceedings; and

- The respective case and underlying facts in detail, providing meaningful and viable documents as well as convictions that would not be mentioned in a police clearance certificate because they fell short of the relevant degree of penalty.

800. In addition, the BaFin is authorized at its discretion to demand further information and documents if this is deemed necessary for assessing trustworthiness and reliability. Specifically, the BaFin requires a complete curriculum vitae (full personal details and description of professional situation) and an updated police clearance certificate in connection with previous convictions and any previous self-employed business.

801. The BaFin must refuse the license if facts are known which indicate that the holder of a qualified participating interest is not trustworthy or fails, for other reasons, to satisfy the requirements relating to the sound and prudent management of the institution (for example, criminal record linked to offenses against property, or legal regulations, especially in the field of business and trade law, competition law or tax law). Furthermore, the BaFin has the power to refuse the license if there is evidence to suggest that the funds raised in order to purchase the qualified participating interest have been acquired by an action which objectively constitutes a criminal offense.

802. An institution applying for a license must submit details about the background and qualification of its managers and directors. Business managers are those natural persons who are appointed by law, articles of association or partnership agreement to manage the business of, and represent an institution organized in the form of a legal person or partnership. The same set of information required for controlling shareholders, must be submitted by the business managers, and the same powers can be exercised by the BaFin in order to require further information and to refuse authorization to take up the management position. At the time of the on-site visit, the BaFin was not assessing trustworthiness and professional qualification of members of the supervisory board (*Mitglieder des Aufsichtsrats*) because they are not included in the definition of senior managers. Amendments to the Banking Act and to the Insurance Supervision Act have since added provisions that require fit-and-proper tests for members of supervisory boards. The amendments entered into force on August 3, 2009. There is no requirement to review automatically all existing supervisory board members and this is only applied on an exceptional basis.

803. Although there is no equivalent fit and proper provision within the Investment Act, the BaFin has applied an administrative practice since 2007, which requires the submission of fit and proper data<sup>68</sup>. It is not clear to the assessors whether the BaFin has the legal authority to prevent the appointment of, or remove unacceptable individuals in all cases. However, the authorities are firmly of the opinion that such authority does exist through their administrative procedures.

804. Once a license has been granted, the BaFin can exercise the same powers with respect to controlling shareholders, business managers, and members of the supervisory board. Institutions, their management, and holders of a qualified participating interest must report immediately to the BaFin the appointment of a new business manager, new member of the supervisory board, and acquisition or disposal of a qualified participating interest. Such changes are then subject to the same approval process.

805. Credit institutions, financial services institutions, and insurance undertakings domiciled in another state of the EEA may provide financial services in Germany either through a branch or subsidiary without a license from the BaFin, provided that: such undertaking is licensed by the competent authorities of such state; the business it conducts in Germany is covered by such license; and the undertaking is

---

<sup>68</sup> Notice on the content of notifications regarding the appointment of members of the supervisory board of investment companies and investment stock corporations, June 15, 2007, reference number: WA 42/09-6 (published on BaFin's website)



supervised by the competent authorities in accordance with regulations which comply with the relevant Directives issued by the European Commission (the so called “European passport”). In such cases, the BaFin does not carry out fit and proper tests on holders of a qualified participating interest, business managers, or members of supervisory boards, nor does it have the authority to order the dismissal of local managers and directors if they are neither trustworthy nor professionally qualified. However, under the European passport arrangements, the BaFin must exercise supervision for AML/CFT of the local branch operations. To do this, the BaFin can and does exchange related information on the basis of the relevant directives or of a specific MOU with the home supervisory authority, which is responsible for prudential supervision of such institutions throughout the EU.

***Ongoing supervision: Regulation and Supervision of Financial Institutions (c. 23.1); Application of Prudential Regulations to AML/CFT (c. 23.4); Monitoring and Supervision of Value Transfer/Exchange Services (c. 23.6); AML/CFT Supervision of other Financial Institutions (c. 23.7); Guidelines for Financial Institutions (c. 25.1):***

806. As indicated above, the BaFin has concentrated its AML/CFT supervisory responsibilities within the MLPG. Therefore, the following description addresses primarily the role and procedures of this group, although the liaison with the Prudential Supervisory Directorate of the BaFin is also noted where relevant. Since the external auditors play an integral part in the ongoing AML/CFT supervisory process and in setting the BaFin’s own agenda, an initial discussion of their responsibilities is necessary.

807. The external auditors of financial institutions supervised by the BaFin and the *Länder* play a pivotal role in the approach to supervising financial institutions for compliance with AML/CFT requirements. First, they produce annual AML/CFT audit reports for all supervised institutions under a specific statutory authority and provide that report to the BaFin. Second, they can carry out specific on-site AML/CFT inspections at the behest of the BaFin. Under Section 340k of the German Commercial Code, all financial institutions subject to the BaFin or *Länder* supervision are required to have their financial statements audited annually, to the standards prescribed by the German Auditors Association. The German Commercial Code specifies the qualifications for the external auditors. As noted in more detail below, external auditors are either independent accounting firms (commercial banks and insurance undertakings), or members of auditing associations (“*Prüfungsverbände*”) associated with the regional associations of banks in the cooperative and savings bank sectors. The rules applicable to the annual audit include a requirement to audit all financial institutions for AML/CFT compliance.

808. Specifically, under Section 29(2) of the Banking Act, the external auditors of credit institutions and financial services institutions are required to examine whether such institutions have complied with their AML obligations under the AML Act, the Banking Act, and EC Regulation 1781/2006 (relating to wire transfers). However, the foregoing obligation does not apply to branches of such institutions from other member states of the EEA, which includes all member states of the EU. Under Section 30 of the Banking Act, the BaFin is authorized to instruct individual financial institutions as to the scope of the external auditors’ work if it considers that the statutory scope needs refocusing or amending in individual cases. It may also require thematic issues to be addressed across the board in the course of the audit.

809. Under sections 5 and 17(1) of the Auditors Report Regulation for Credit Institutions and Financial Services Institutions (hereinafter referred to as the Auditors Report Regulation), the auditors must address a broad range of AML/CFT and related requirements, specifically:

- The filling of the senior executive positions (including the ML compliance officer) within the meaning of the AML Act and their deputies, their position in the organizational structure of the financial institutions, and any changes made;



- The identification requirements of the Tax Code;
- The identification of the economic beneficiary (the beneficial owner);
- The recording and preservation requirements;
- The obligation to report suspicious transactions;
- The creation of an internal system for reporting suspicions;
- Internal reports on suspicious cases made during the period under review; and
- The STRs filed with the LKAs with copies filed with the FIU, and the accounts closed and customer relationships terminated as a result of suspicion of ML transactions.

810. Under Section 17(2) of the Regulation, the internal monitoring systems have to be discussed and assessed, especially:

- The activities of the compliance officer during the period under review;
- The principles, procedures, and security systems to prevent ML which the institution has evolved for transactions and for business that is judged to be risky in terms of ML, and the changes made to these principles etc. during the period under review;
- The nature and frequency of briefings of the institution's staff on ML methods that have come to light;
- The precautions taken by the appropriate office of the credit institution to file STRs;
- The internal audit division's audit activities and their results (number and nature of the findings); and
- An assessment of whether the internal audit division's audit work in compliance with their obligations was adequate, whether written reports on this monitoring were prepared, and whether these reports were submitted to the executive board.

811. The same system of external audit reports is also required for prudential supervisory purposes, pursuant to Section 29(1) of the Banking Act.

812. The AML/CFT audit report does not form part of the formal audit opinion, which remains linked purely to the financial position of the institution. The report must be filed within three months of the financial year-end (mostly end-December for German banks); but in the event that the auditors find serious failings, they are obliged under Section 29 of the Banking Act to report the facts immediately to the BaFin, which may require the auditors to provide further information (similar provisions apply to institutions governed by the Investment Act and the Insurance Supervision Act). In such cases, the auditors are given statutory protection from any potential breaches of professional secrecy.

813. While the specific areas to be covered in the audit are laid down in the Auditors Report Regulation, there are only limited agreed procedures or auditing standards for the work. Moreover, the regulations have now been outdated by the new AML Act and the introduction of the risk-based approach.

The authorities indicated that there are plans to update the Auditors Report Regulation, but at the time of the on-site visit, discussions to this end had been ongoing for some time, without resolution.<sup>69</sup> To some extent, the auditor sector has taken the initiative by publishing articles and checklists in the German audit journal, describing what they see as the proper process to be followed in completing the process under the new legislation. The private commercial banks and the insurance undertakings choose their own external auditors, who are formally appointed by their shareholders. The savings banks and the cooperative banks, however, are all members of regional banking associations which provide various common services to all members, including external auditing services through corresponding regional auditing association. In these latter cases, the institutions have no discretion as to the appointment of their auditors. There are a total of 18 of these regional auditing organizations: 7 for the cooperative banks and 11 for the public sector savings banks. Together, the regional auditing associations provide external auditing services to approximately 1 700 institutions, or more than 80% of all banks in Germany, accounting for more than 75% of all assets in the banking sector.

814. Notwithstanding the different arrangements for external auditing in these sectors, the auditors interviewed by assessors confirmed that the professional standards (educational qualifications, auditing standards, etc.) applied by the auditing associations' auditors are the same as those of the independent external auditors used by the private commercial banks.

815. The BaFin requires all auditors to provide it with a copy of their annual audit reports described above, and this becomes a central element in the BaFin's AML/CFT supervisory framework, which is in a stage of transition. In 2006, the BaFin adopted a risk-based approach to its AML/CFT supervisory program, consistent with its approach to prudential risk generally. Under this approach, the BaFin allocates the highest levels of AML/CFT supervisory attention to the financial institutions exhibiting the highest levels of assessed net risk as evidenced by the information provided in the auditors' reports.

816. The BaFin reads at least the Executive Summary of every audit report. In order to assess the net risk profile, financial institutions are first analyzed by the BaFin and rated (low, average or high) against five essential inherent risk criteria:

- Location (*e.g.* criminal areas, business areas)
- Scope of business (regional, national, international)
- Product structure (*e.g.* money remittance, private banking)
- Customer structure (*e.g.* nonresidents, PEPs)
- Distribution structure (*e.g.* branches, brokers, online-services).

817. Next, the quality of an institution's AML/CFT measures and safeguards, as described in its audit report, is assessed and rated by the BaFin, based on compliance with three categories of responsibility: "internal safeguards," "customer due diligence" and "other duties." For the rating, several individual criteria are checked, which vary only slightly by sector. Certain categories of control criteria are assigned different weights in establishing the resultant risk matrix because non-compliance with them has a more significant impact on the overall AML regime. For example, the categories relating to the role of the Money Laundering Compliance Officer, transaction monitoring and understanding the customer's business are especially important in establishing the resultant risk matrix depending on the sector.

---

<sup>69</sup> The regulation was passed and came into effect on November 26, 2009.

818. For the purpose of the final net risk classification, the BaFin assigns each entity ratings based on inherent risk and quality of controls, which in turn drives a net risk. These range from 1A (low risk-high quality of controls) to 3D (high risk–low quality of controls), and are summarized in Section 1 of this report. A breakdown of the classifications by sector is set out in the following tables.

**Statistical Table 21: AML/CFT Risk Profiles of Credit institutions on the basis of the evaluation of reports of 1 353 out of 2 048 institutions**

		Quality of AML/CFT-prevention			
		A (high)	B (medium-high)	C (medium-low)	D (low)
Potential threat of ML/TF	3 (high)	2%	2%	<1%	<1%
	2 (medium)	71%	10%	2%	1%
	1 (low)	13%	1%	<1%	<1%

**Statistical Table 22: AML/CFT Risk Profiles of money remittance services and currency exchange on the basis of evaluating 42 out of 57 annual audit reports**

		Quality of AML/CFT-prevention			
		A (high)	B (medium-high)	C (medium-low)	D (low)
Potential threat of ML/TF	3 (high)	-	5%	2%	7%
	2 (medium)	31%	33%	7%	-
	1 (low)	7%	5%	-	2%

**Statistical Table 23: AML/CFT Risk Profiles of financial services institutions (other than those under Table 2) on the basis of the evaluation of reports of 635 out of 720 institutions.**

		Quality of AML/CFT-prevention

		A (high)	B (medium-high)	C (medium-low)	D (low)
Potential threat of ML/TF	3 (high)	<1%	-	-	-
	2 (medium)	37%	28%	4%	<1%-
	1 (low)	11%	17%	3%	2%

Statistical Table 24: AML/CFT Risk Profiles of insurance undertakings (life insurance and accident insurance with premium redemption) on the basis of the evaluation of reports of 117 out of 134 institutions

		Quality of AML/CFT-prevention			
		A (high)	B (medium-high)	C (medium-low)	D (low)
Potential threat of ML/TF	3 (high)	-	<1%	<1%	-
	2 (medium)	21%	33%	4%	-
	1 (low)	11%	27%	3%	-

819. The above ratings are based purely on the assessed AML/CFT net risk and do not include any broader prudential aspects. The MLPG liaises with the BaFin's Prudential Supervisory Directorates to ensure they have an understanding of the AML/CFT net risk profile, which feeds directly into the prudential supervisors' larger perspective. However, the MLPG operates independently of prudential supervision. The BaFin advised the assessors that prudential weaknesses could trigger an assessment by the MLPG as to whether similar weaknesses exist in AML/CFT controls; but in general, prudential weaknesses do not have an effect on the analysis of the AML/CFT situation.

820. Broadly, the ratings produced by the MLPG result in three levels of AML/CFT supervision:

- Simplified basic supervision for low-net risk entities (1A, 1B and 2A). At a minimum, the BaFin applies sufficient supervisory attention to ensure an adequate response to any identified medium or high-risk findings;
- Basic supervision for medium-net risk entities (rated 1C, 1D, 2B, 2C, 3A and 3B). These institutions will generally be subject to a basic supervision plan, such as requiring a timetable for

corrective measures, transmitting a copy of an internal audit report certifying that appropriate corrective measures have been taken, or both;

- Enhanced supervision for high-net risk entities (rated 2D, 3C and 3D). These institutions receive the highest degree of supervisory attention. This will usually take the form of:
  - Several phone calls and letters exchanged to make sure that corrective measures are taken and that these measures are adequate, timely, and ultimately successful;
  - Ordering regular reports;
  - Supervisory visits (“special audits” or “audit accompaniments”); and
  - Summoning management to the BaFin.

821. Due to their inherently higher risk for ML/TF, large credit institutions receive at least a medium or even a high level of supervision; a category 3 institution cannot qualify for the lowest level of supervision.

822. The BaFin advised that in the case of branches of financial institution domiciled in other member states of the EEA and subject to the European Passport arrangement (which does not include the provision of external auditors’ reports to the BaFin), the BaFin applies compensatory supervisory measures to obtain information on their compliance with AML/CFT requirements. These measures include holding meetings with such branches on a rotating basis, supported by meetings with the foreign banks industry association regularly and at least annually; and requests to these branches to provide the BaFin with the results of spot checks and internal audit reporting to the extent these cover AML/CFT requirements. In addition, the BaFin can initiate special audits (described below) where there is reason to believe there are shortcomings, and also receives information from the home EEA supervisors, if need be. There are 96 branches of EEA financial institutions located in Germany.

823. According to the Banking Act, branches of German financial institutions domiciled abroad are included in consolidated supervision and, hence, are subject to the annual report of the auditors as described above. Subsidiaries, although not included in the consolidation, are also subject to this requirement. There are 331 branches and subsidiaries of financial institutions outside Germany located in 50 jurisdictions, of which 26 are EU or EEA states. The BaFin advised the assessors that in the two years preceding the on-site visit, the BaFin has conducted two on-site visits to such branches, one in Austria and one in Switzerland.

824. Based on the application of the foregoing compliance rating system started in 2007 and not yet completed as noted above, only a small percentage of financial institutions are subject to the highest degree of attention (Group 2D, 3C and 3D), as shown in the following table, with the other groups shown for comparison purposes. However, it is ensured that the credit institutions with the highest inherent risk (category 3) receive at least a medium or even high level of supervision, because a category 3 institution cannot qualify for the lowest level of supervision.

Types of institution	Percentage of supervised institutions		
	Lowest level of Supervision (Group 1A, 1B, 2A)	Middle Level of Supervision (Group 1C, 1D, 2B, 2C, 3A and 3B)	Highest Level of Supervision (Group 2D, 3C and 3D)
Credit institutions	84%	15%	1%
Remitters and foreign exchange	43%	48%	10%
Financial services institutions	64%	36%	<1%
Insurance companies	58%	41%	1%

(Note: numbers may not add to 100% due to rounding).

825. The BaFin has powers to commission its own audits at financial institutions. These are referred to as “special audits” to distinguish them from the annual audits performed by the external auditors. The BaFin has authority to use the services of third persons in order to perform its duties. In the case of credit institutions, the BaFin normally instructs the institutions’ external auditors to carry out these special audits; in the case of insurance undertakings and other financial services institutions (including money remitters and currency dealers), the audits are usually led by the BaFin. This is because, prior to the merger of the predecessor supervisors, the insurance supervisor led all on-site work in that sector. Although the auditors are accountable to the BaFin for the special audits, they are not authorized to issue orders or to take supervisory measures, which are the sole prerogative of the BaFin. Special audits are made regularly at institutions that attract the highest level of supervision.

826. The following table sets out the numbers of special audits made over the past few years (keeping in mind that the present net risk grading system only came into effect in 2007).

Year	2003	2004	2005	2006	2007	2008
Credit institutions	23	18	23	18	14	8
Money transmission services, currency exchange and credit card businesses	-	2	5	7	4	7
Insurance undertakings	-	1	3	2	3	3
Capital investment companies and stock investment corporations	-	-	-	-	-	-
<b>Total</b>	<b>23</b>	<b>21</b>	<b>31</b>	<b>27</b>	<b>21</b>	<b>18</b>

827. The BaFin also conducted 17 “audit accompaniments” in 2007 and 14 in 2008. Eleven are planned for 2009. The content and purpose of audit accompaniments is essentially the same as special audits, although the primary objective is to get a picture of the AML/CFT situation and to undertake routine sampling of the quality of the basic audit work. These audit accompaniments are also led by the external auditor, not the BaFin, but, unlike the special audits, they do include staff from the BaFin’s MLPG.



828. In summary, a total of 38 on-site visits of both types were conducted in 2007 and 32 in 2008.

829. The BaFin does not analyze in depth all the audit reports received in a given year; however, as noted above, it does review, at a minimum, all the content of the executive summaries of such reports. In 2008, it analyzed in detail 1 182 reports, out of a total of 3 203 institutions under supervision in the same period. The BaFin has advised the assessors that, with effect from 2007 (under its new risk-based approach) due to resource constraints it aims to review the reports for the larger institutions annually, with those of the smaller institutions being actively reviewed about every three years. For the small cooperative and savings banks, it has also taken the decision not to receive all reports each year, but to take half in alternate years.

830. From the foregoing description it is readily apparent that the BaFin's AML/CFT supervisory approach is heavily dependent on the work of the auditors and, similarly, on the ability of the BaFin to analyze effectively the strength of the institutions' AML/CFT controls is highly dependent on the quality of the content of the reports. From a review of a sample of these reports provided by the BaFin, it was apparent that there was a wide variety in the scope and depth of analysis provided, especially with respect to the assessment of the CFT measures. The most noticeable difference in content was in the sampled reporting by the auditing associations of the regional cooperative banks, which did not appear to the assessors to be as comprehensive as the reports submitted by independent external auditors in the private commercial bank sector. Although the authorities confirmed that the Chamber of Auditors has established generally accepted auditing standards applicable to the AML/CFT audits, any difference in the quality of reports potentially weakens the BaFin's overall supervisory approach, especially given the large size of these sectors as noted above. It is understood that the BaFin has sought to engage the auditing associations of the cooperative banks on this issue, but there has only been limited success in bringing about improvements.

831. As regards the insurance undertakings that fall outside the BaFin's remit, the processes followed are understood to be similar to those of the BaFin. In addition, the Lower Saxony regulatory authority advised that they regularly meet with the two insurance undertakings, including the management board and the chief auditor. If there is further need for clarification on matters of regulatory law, technical discussions are held with the undertaking's directors, the persons monitoring the company, or both.

832. The BaFin has issued guidelines and circulars on a selective basis, over the years, in order to inform the financial sector about its administrative practices in some areas, and to assist supervised entities in interpreting and implementing the provisions of the AML Act. Until the emergence of the ZKA guidelines (see section 3.1. above), the key document was the circular of March 30, 1998 concerning measures to be taken by credit institutions to combat and prevent ML. There were also similar circulars for other sectors. For the reasons noted at the beginning of Section 3 above, in early-2009, the BaFin abrogated a considerable part of its guidance papers and circulars, while, at the same time, notified the institutions that such abrogated guidance would continue to provide a basis for its supervision (administrative practice), wherever they do not conflict with the new legal provisions. This has caused confusion within some parts of the financial sector.

833. The new ZKA guidance is focused mainly on those aspects that are new under the 2008 AML Act, including how financial institutions should implement the risk-based approach. It is not fully rolled out nor comprehensive in its coverage (due to time constraints caused by the later-than-expected enactment of the new law) and the ZKA anticipates publishing an expanded version in 2010. The BaFin and the MoF have formally endorsed the ZKA guidance, and, by so doing, the BaFin has indicated that it will use the ZKA guidelines as the basis for its administrative practices (supervisory measures). A similar process was followed in the insurance undertakings sector, where the German Insurance Association (GDV) published its own specific guidance (also endorsed by the BaFin). Finally, the Association of Building Societies and

the Federal Headquarters of State Building Societies (subgroupings of banking entities) has taken similar action.

834. Supervision of financial institutions in Germany is concentrated at the federal level through the BaFin. However, the insurance intermediary sector and three small public sector insurance undertakings are regulated by the *Länder*. As it was impracticable to interview all 16 *Länder* authorities, assessors chose to interview the authorities in the federal *Land* of Hesse for the purpose of assessing *Länder* supervision of insurance intermediaries and financial enterprises. The territory of Hesse includes the city of Frankfurt, which is Germany's foremost financial center, and for this reason the assessors felt this would provide a reasonable profile of *Land* supervision of insurance intermediaries and financial enterprises. In Hesse, the competent authority for supervising insurance intermediaries and financial enterprises is the Chamber of Industry and Commerce, which is supervised by the Hesse Ministry of the Economy. One of the Chamber's principal functions is to deploy the *Land* licensing regime applicable to insurance agents and brokers, which can be natural persons or legal persons. However, the authorities appeared to be relatively unfamiliar with the AML/CFT requirements and appear to have significant resource shortages to apply to their responsibilities to enforce the AML Act in the insurance intermediaries sector.

835. The *Länder* authorities have not issued any guidance applicable to the 72 000 insurance intermediaries in Germany.

### **Effectiveness of implementation**

836. Overall, the statutory powers provided to the BaFin appear to be wide-ranging and appropriate. The reliance-based methodology used by the BaFin starting in 2003 appears to have served the BaFin well in the rules-based AML/CFT framework in place prior to 2008. As noted in more detail below, however, the assessors believe that the advent of the risk-based approach, coupled with the relatively low number of on-site visits in which the MLPG participates, suggests that the BaFin should modify its approach to on-site supervision, specifically to include more financial institutions showing higher inherent risk profiles. In turn, this may have an impact on resources. In addition, the auditing standards may need to be reviewed to ensure that auditors have appropriate means to determine whether the risk-based measures adopted by banks are compliant with AML/CFT requirements.

837. Although the role of the *Länder* authorities in AML/CFT is limited to supervising insurance intermediaries, the assessors did not get a clear picture of their overall approach to supervision of these entities, aside from noting that the resources assigned to supervision seem to be low when compared to the approximate 72 000 insurance intermediaries in Germany.

### **Recommendation 17**

838. There are relatively few violations of the AML Act which attract specific administrative fines. The assessors were told this is driven by the German legal principle of specificity coupled with the fact that administrative fines are criminal in nature. However, the FATF standards apply whether sanctions are based in criminal law or otherwise. Moreover, it is noteworthy that, for example, no administrative fines apply for failures to gather specific information on natural persons or legal persons who are the contracting party; to obtain information on the purpose and intended nature of the business relationship; to continuously monitor the business relationship, all of which contain a degree of specificity equivalent to violations which do attract administrative fines.

839. The administrative fines which carry higher penalties can be applied in the case of violations caused by gross negligence or deliberate intent. These include basic failures to collect client data or

complete records. However, lower penalties are applied against more serious breaches, including failure to identify the beneficial owner. Moreover, these cannot be applied other than in cases of deliberate intent.

840. The relatively low levels of available administrative fines generally, and especially those resulting from serious violations such as failure to identify the beneficial owner, are not dissuasive, particularly as none have been applied and also taking into account the very large size of many German banks and other financial institutions and groups (although this approach is consistent with the Administrative Offenses Act which contemplates low levels of fines for offenses generally (*i.e.* where not specified in individual legislation)).

841. The BaFin has only ever imposed one administrative fine for a violation of the (previous) AML Act. The *Länder* authorities have never imposed a fine for the violations set out in the AML Act. The BaFin has only ever issued two supervisory instructions relevant to AML/CFT under the Banking Act, in 2005 and 2009, respectively. The BaFin was aware of only two or three cases over the last five years where suspicious activity came to its attention which should have been reported to the authorities by financial institutions. Such omissions specifically attract administrative fines under the AML Act, but did not attract an administrative fine under the old AML law. Neither the BaFin nor the *Länder* authorities have ever issued any orders or dismissed any managers under Section 87 of the Insurance Supervision Act.

842. Administrative payments are not administrative fines and are used to enforce supervisory measures. They can only be applied indirectly for failures to comply with the AML Act. They are, therefore, an acceptable form of sanction, so long as there is a practice of using them for failure to comply with AML/CFT requirements.

843. Supervisory letters are the basic regulatory compliance tool and are issued, *inter alia*, where the external auditors identify instances of noncompliance with AML/CFT requirements. If no action is taken, a second, or warning, letter is issued by the BaFin. As noted above, the BaFin has imposed very few such warnings (14 in 2008 compared to a total of 3 452 supervised institutions). Given the very large size of the German financial sector and the significant numbers and types of financial institutions in the sector, the assessors believe it is unlikely that there is such a very high level of compliance with AML/CFT measures that the very small volume of warnings and related threats of administrative payments would suggest, including the absence of any recently applied administrative payments (administrative fines cannot result from failure to comply with warning letters).

844. The BaFin has used the threat of dismissal twice in the past few years: in one case, following a year-long investigation, a member of a bank's board of managers was warned, but resigned before he could be dismissed. The other case involved the identification of serious deficiencies in a financial institution's internal safeguards in respect of two customers. Following an investigation, the BaFin issued letters of warning to two members of the institution's management board. However, as noted above, had the institution failed to comply with the warning, only an administrative payment (and not a fine) were available, which according to the authorities are not designed to be punitive. For these reasons, the assessors have doubts about the enforceability of dismissal as an AML/CFT sanction.

845. The BaFin argues that it is rarely necessary to consider the application of direct sanctions (*i.e.* administrative fines) under Section 17 of the AML Act, because the threat of the use of its powers against management under the sector laws (*i.e.*, administrative payments) is sufficient to bring about compliance. It believes that there is a fine line to be drawn between the application of sanctions and the use of preventive measures. The assessors' view, however, is that administrative payments have seldom been applied in practice; that the number of on-site inspections involving the BaFin staff directly is too low to assess the effectiveness of the BaFin's strategy, and is itself an indicator of lack of effectiveness; and in any event, the AML Act administrative fines cannot be used to enforce supervisory measures.

846. The specific administrative fines set out in the AML Act address violations associated with the implementation of CDD and reporting measures. These measures would be implemented by managers or the management board and not by members of the supervisory board. The assessors believe that the threat of financial penalties against members of the supervisory board for management's AML/CFT compliance failures would more directly address effectiveness of implementation of the "internal safeguards" by management, because the supervisory board is responsible for effective oversight of management.

847. In summary, there are issues about the effectiveness (proportionality, dissuasiveness) of sanctioning powers in place. The BaFin prefers to rely more on the concept of "moral suasion" as evinced through its supervisory process (administrative practices). Moreover, the concepts of "specificity" and "certainty" in German criminal law that define the circumstances in which administrative fines can be effectively applied, militate to a significant extent against the use of administrative fines, given the limited range of specified offenses. In turn, this raises the overall question of whether the sanctioning structure of administrative fines is sufficiently enforceable. Furthermore, the migration to a risk-based approach, which is now embedded in the AML Act, is likely to exacerbate the issues of specificity and certainty, since there may be no clear benchmark against which to judge the specific degree of noncompliance required under the law before formal actions can be taken.

### ***Recommendation 23***

848. The BaFin MLPG appears to be knowledgeable and proficient with respect to AML/CFT legislation and the obligations of their supervised financial institutions. The BaFin's supervised sector is very large, with nearly 3 500 institutions under supervision as of February 2009. The total number of the BaFin staff assigned directly to AML/CFT monitoring and supervision is 47.5 FTE, resulting in a ratio of about 73 financial institutions per FTE. This ratio suggests a lack of resources. In particular, the unit of the BaFin's MLPG, which supervises more than 2 000 credit institutions, has only 14 staff, or a ratio of about 150 entities per FTE. This is a very high ratio. The ratio may reflect the German system of obtaining some supervisory information from external auditors, and may also explain why the BaFin applies a light AML/CFT supervisory touch in many cases. This lack of resources, coupled with the deficiencies relating to sanctions, impacts the overall effectiveness of AML/CFT supervision.

849. The BaFin relies systemically on the work of the auditors, and restricts direct supervisory intervention on AML/CFT matters to a very small number of institutions exhibiting the highest net risk profile (inherent risk, mitigated by quality of controls). Even when "audit accompaniments" are included, the numbers of institutions where the BaFin intervenes directly is very low. Although this approach helps the BaFin allocate limited supervisory resources, it does not enable it to directly assess the controls of institutions where ML/TF risk is rated as inherently higher, other than through the work of the auditors. The ability of the BaFin and auditors to assess the quality of risk management and reasonable measures under the risk-based approach are now much more significant than in the past. Controls are likely to differ more than at present among various banks and may not lend themselves to the systematic analysis by external auditors under the previous rules-based approach to compliance. If the BaFin could expand on-site supervision to include more credit institutions exhibiting higher risk levels, it would have firsthand knowledge about controls developed by these institutions and be able to provide better input into the guidance process.

850. The BaFin is aware of the need for more engagement with the auditing profession and has been engaged in bilateral and industry discussions with the IDW and one regional auditing association. The AML Act took effect in August 2008, and therefore auditors' reports on the first full year's implementation by the financial sector of the risk-based approach will not be available to the BaFin for analysis until 2010. Thus, no information was available to the assessors on the authorities' overall evaluation of the new requirements.

### ***Recommendation 25***

851. The move to a risk-based approach, generally, is presenting many institutions and the BaFin with significant new challenges. Key elements in the transition are for institutions to gain a better understanding of how the BaFin sees this approach developing in practice, and how it will interpret the requirements through its regulatory processes; and for the BaFin to ensure that the auditors move to a more risk-based assessment. Therefore, it is important that the BaFin should engage in significant outreach in order to educate the smaller banks, in particular. The decision taken to abrogate most of the BaFin's guidance, while at the same time stating that such guidance would remain in effect unless it clashed with the new AML Act, has caused some confusion, notwithstanding the private sector's efforts to introduce its own guidance (endorsed by the BaFin).

852. The German authorities have not issued comprehensive guidance to the approximately 72 000 insurance intermediaries despite there being specific German typologies in place indicating that one of two suspected Al-Qaida terrorists planning suicide bomb attacks had taken out life insurance in Germany in 2004 and was planning to fake his own death to raise funds for the attacks. However, the GDV guidance (endorsed by the BaFin) in the insurance undertaking sector may address key issues for these intermediaries.

### ***Recommendation 29***

853. The BaFin has adequate prudential supervisory powers, and the AML Act allows it to use these to monitor and ensure compliance with AML/CFT requirements by financial institutions. The AML Act also authorizes the BaFin to apply the administrative fines contained in the AML Act. The BaFin sets its own budget and has the ability to assess the financial sector for the necessary funding to ensure that its supervisory objectives can be met. The assessors did not review the entire universe of prudential supervision by the BaFin, but were informed that the overall approach used by the MLPG is fairly representative of the BaFin's overall approach to supervision.

854. The systematic receipt and evaluation by the BaFin of the external audit reports is a valuable and comprehensive way of monitoring how financial institutions implement compliance with the AML/CFT requirements. However, there are concerns about the depth and breadth of these reports, particularly in certain geographical areas in the cooperative banking sector. Finally, auditing standard changes applicable to the current AML Act, especially relating to the implementation of the risk-based approach, mean that there need to be changes in the methodology to ensure the audit reports can continue to be relied on by the BaFin.

#### ***3.10.2. Recommendations and Comments***

855. In order to comply fully with Recommendations 17, 23, 25, and 29, Germany should:

- Add specific administrative fines for AML violations into the Insurance Supervision Act and the Investment Act.
- Increase the range of specific administrative fines under the AML Act and also lower application thresholds (negligence or deliberate intent).
- Increase the amounts of specific administrative fines under the AML Act for the more serious violations set out in Section 17(2) of the AML Act, and extend their applicability to gross negligence.



- Ensure that members of the (supervisory) Board of Directors are explicitly subject to appropriate administrative fines for failure to supervise managers responsible for compliance.
- Introduce legal provisions that explicitly allow the BaFin to dismiss managers and members of (supervisory) Boards of Directors for AML/CFT violations.
- Review the adequacy of the frequency with which the high-risk institutions are subject to on-site inspection by the BaFin and the consequential impact on resources.
- Address the issue of guidance on audit report quality as a priority with the auditing organizations in the cooperative banking sector.
- Ensure that *Länder* authorities are sufficiently aware of their AML/CFT supervisory responsibilities and apply sufficient resources to supervise insurance intermediaries.
- Arrange for *Länder* authorities to issue guidance to insurance intermediaries.

### 3.10.3 Compliance with Recommendations 17, 23, 25 & 29

	Rating	Summary of factors underlying rating
R.17	PC	<ul style="list-style-type: none"> <li>• Administrative fines in place are not proportionate (very low number of administrative fines available under the AML Act) nor sufficiently dissuasive (more serious violations of the AML Act attract lower levels of administrative fines); and the maximum amounts of fines under the AML Act are low (especially considering the large size of many German financial institutions); and, due to the criminal nature of the penalties, high penalties can only be applied for gross negligence or deliberate intent).</li> <li>• Administrative fines are not applied effectively — the BaFin has only ever applied one administrative fine many years ago.</li> <li>• Due to the constitutional principle of specificity, there are no administrative fines for violations of obligations to establish appropriate internal safeguards under all sector-specific laws; and apply enhanced due diligence in specific additional circumstances listed in the Banking and Investment Acts.</li> <li>• Failure by the supervisory boards to comply with their obligation to supervise management may result in uncertainty as to whether administrative fines apply to individual members of such boards.</li> </ul>
R.23	LC	<ul style="list-style-type: none"> <li>• Uncertainty about the legal basis for the BaFin's ability to apply fit and proper testing for members of supervisory boards of investment companies.</li> <li>• Lack of effectiveness in aspects of supervisory practice: <ul style="list-style-type: none"> <li>○ Lack of effective sanctions for noncompliance with AML/CFT requirements.</li> <li>○ Issues about uncertain quality of audit reports for some cooperative banks; AML/CFT auditing standard had not been updated.<sup>70</sup></li> <li>○ <i>Länder</i> authorities seem unfamiliar with their AML supervisory responsibilities and appear to apply insufficient resources to supervise a large number of insurance intermediaries.</li> <li>○ Fit and proper requirements for supervisory board members have not been applied to existing board members due to the newness of the requirements.</li> </ul> </li> </ul>
R.25	PC	<ul style="list-style-type: none"> <li>• Uncertainty in some parts of the financial sector on the status of abrogated circulars.</li> <li>• New (replacement) private sector guidance (approved by the BaFin and the MoF) is</li> </ul>

<sup>70</sup>

Regulations were issued on November 26, 2009 to address this issue (albeit outside the 2 months timeframe mentioned in the FATF Handbook for countries and evaluators).



	Rating	Summary of factors underlying rating
		<p>limited in scope.</p> <ul style="list-style-type: none"> <li>Lack of comprehensive guidance in place for the insurance intermediaries sector.</li> </ul> <p>Rating for this section: <b>PC</b></p>
<b>R.29</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>Although the BaFin has adequate supervisory powers, there are weaknesses in respect of the effective use of such powers in practice.</li> <li>Fit and proper requirements for supervisory board members have not been applied to existing board members due to the newness of the requirements.</li> </ul>

### 3.11. Money or Value Transfer Services (SR.VI)

#### 3.11.1. Description and Analysis (summary)

##### *Designation of Registration or Licensing Authority (c. VI.1); Adequacy of Resources – MVT Registration, Licensing and Supervisory Authority (R.30)*

856. In Germany, MVTS providers are “financial services institutions” as defined in Section 1(1a) of the Banking Act. Such services include “the execution of payment orders (money transmission services).” MVTS providers have been supervised by the BaFin since 1998. At the time of the on-site visit, there were 39 licensed money remitters in Germany, in addition to the banks which also provide such services.

857. MVTS operators are licensed under the Banking Act in the same manner as banks and other financial services institutions. The licensing procedure is undertaken by the BaFin, and there are key conditions for the granting of such licenses, including sufficient capital and business resources, organizational requirements, and “fit and proper” requirements applicable to owners and senior managers. The head office of the financial service businesses licensed by the BaFin must be located in Germany. Under Section 33(1) of the Banking Act, money remitters cannot be operated as sole proprietorships. Hence, natural persons may only operate money remittance businesses in Germany if they are members of a partnership company. The BaFin has statutory authority to make the granting of licenses subject to conditions, which must be consistent with the purpose pursued by the Banking Act, and it may limit the license to certain types of businesses, including geographical restrictions (*e.g.* limits on sizes of transfers to particular jurisdictions to deter the “financial agents” phenomenon).

858. The BaFin has issued guidance (“Requirements for the granting of a license to provide money transmission services pursuant to Section 1(1a) sentence 2 no. 6 of the German Banking Act”) on the application and licensing process, most recently updated on February 21, 2008. This guidance simply interprets the legal requirements and does not add enforceable obligations (see the discussion on OEM above).

859. Pursuant to Section 33 (1) of the Banking Act, the BaFin must refuse to grant a license in the following circumstances:

- facts are known which suggest that an applicant or its managers is not trustworthy;
- facts are known which warrant the assumption that the holder of a qualified participating interest or, in the case of a legal person, a legal representative or representatives according to the articles of association or, in the case of a partnership, a general partner is not trustworthy or for other reasons fails to satisfy the requirements to be set in the interests of the sound and prudent management of the institution;

- facts are known which suggest that the proprietor or managers do not have the professional qualifications necessary for managing the institution;
- a credit institution or a financial services institution which, in the course of providing financial services, is authorized to obtain ownership or possession of funds or securities of customers does not have at least two managers who work for the institution not merely in an honorary capacity;
- the institution has its head office outside Germany;
- the institution is not prepared or not in a position to make the organizational arrangements necessary for the proper operation of the business for which it is seeking a license; or
- the applicant is a subsidiary of a foreign credit institution and the competent foreign supervisory authority for this credit institution has not given its consent to the establishment of the subsidiary.

860. As a matter of routine, the BaFin will visit a new licensee within four to six months after the license has been issued to verify that the systems and control procedures described in the application have been put into practice. Thereafter, reliance is placed on the annual AML/CFT audit, as for other financial institutions.

861. There are six persons assigned full time in the MLPG to the supervision of money remitters and the enforcement actions against illegal remitters. The BaFin has the authority to enter premises, have access to books and records, seize evidence, and take statements when investigating illicit activity. When such activity is identified, the BaFin issues 'cease and desist' orders, initially orally with a written administrative decision shortly thereafter. If the illegal activity persists following these measures, the BaFin refers the file to the public prosecutor. In 2008, the BaFin investigated 129 unlicensed remitters (171 in 2007). If the illegal activity persists, the BaFin refers the file to the public prosecutor.

862. The BaFin told the assessors that most illegal remittance activity is concentrated among various ethnic groups and is relatively small in volume, although a few years ago, an illegal operator had been shut down whose volume was about EUR 6–7 million per year (USD 8-10 million). The BaFin has investigated between 100 and 200 cases of illegal remittance activity *per annum* in Germany over the past few years, and shuts down around 15 operators each year. Identifying and apprehending this activity requires constant monitoring and pressure. Relatively few illegal operations are initially identified by the police or prosecution (even though they have a legal obligation to report any evidence to the BaFin); most illicit operations are usually identified by the BaFin through scanning open sources or through whistleblowers (especially competitor operations). Illegal operations are most commonly found among travel agents, import-export companies, and small retail outlets.

***Application of FATF Recommendations (applying R.4-11, 13-15 & 21-23, & SRI-IX)(c. VI.2); Monitoring of Value Transfer Service Operators (c. VI.3)***

863. The full range of measures discussed under Recommendations 4 to 11, 13 to 15, 21 to 23 and SRI to IX apply to money remitters, except that, because they are classified as financial services businesses, they are not subject to certain measures which only apply to credit institutions and insurance companies, including, for example, the obligation to have data processing systems which recognize customer relationships. The BaFin told the assessors that suitable data processing requirements are imposed as a condition of granting the license. The remaining exclusions are not material to the overall regime.

***List of Agents (c. VI.4):***

864. All licensed MVT operators file a list of their cooperation partners (staff and managers that run operations) in Germany and abroad. This is a licensing requirement imposed by the BaFin by administrative practice and is also captured as part of the annual audit report process. Maintenance of lists of cooperation partners is not explicitly addressed in the Banking Act or the Auditor Regulations (it used to be but was repealed). The BaFin requires, through regular supervision administrative practice, money remitters to notify it when new cooperation partners are appointed, through a monthly reporting process.

865. In Germany, MVT operators are effectively not permitted to appoint agents by virtue of the provisions of the Banking Act which requires all persons to be directly licensed (including situations where services are only partially provided in Germany). Thus, agents (self-employed traders who carry out transactions under a franchise-type arrangement) are not allowed. All MVT operators are required to settle transactions through regulated credit institutions.

***Sanctions (applying c. 17.1-17.4 in R.17)(c. VI.5):***

866. The range of sanctions derived from the AML Act and sanctions applicable to financial services institutions under the Banking Act (as described under Recommendation 17), and their identified deficiencies, also apply to money remitters.

***Additional Element — Applying Best Practices Paper for SR VI (c. VI.6):***

867. Germany's MVT licensing regime appears to be compliant with the FATF Best Practice paper on SR.VI.

**Effectiveness of Implementation**

868. Germany has a reasonably effective regulatory framework in place for the monitoring of money remitters. However, weaknesses identified in CDD requirements, the STR reporting requirement, and the availability and use of sanctions tend to impact the overall effectiveness of the framework. The assessors have, therefore, taken into account the factors underlying the ratings of Recommendations 5, 13, and 17 in evaluating compliance with SR.VI.

869. The size of the German economy, coupled with high levels of foreign workers, appears to generate high demand for remittance services outside the regular banking sector. The BaFin has an enforcement unit in place (consisting of 6 FTE) which has been identifying and closing down a steady stream of illicit remittance activity since 1998. The consistent volume of illicit activity, at levels significantly higher than licensed activity, seems to suggest that more resources may be needed in this work.

870. No explicit requirement applies (aside from a filing required upon application for licensing and information supplied in the annual audit process) to MVTS operators to maintain lists of their cooperation partners. However, the system in place captures the naming of cooperation partners both at the time of licensing and also annually through the audit report process. From an effectiveness point of view, the assessors are satisfied, given the relatively small number of licensed remitters, that the BaFin can and does obtain updated information and can access this information on demand when needed.

***3.11.2. Recommendations and Comments***

871. In order to comply fully with Special Recommendation VI, Germany should:

- The recommendations and comments applicable to Recommendations 5, 13, and 17 apply, where applicable, to the MVTS sector in accordance with the FATF methodology.
- The authorities should consider applying more resources to identifying and closing illicit money remittance operations.

### **3.11.3. Compliance with Special Recommendation VI**

	<b>Rating</b>	<b>Summary of factors underlying rating</b>
<b>SR.VI</b>	<b>LC</b>	<ul style="list-style-type: none"><li>• Effectiveness: deficiencies in regulations or other measures in the areas of CDD, reporting of suspicious transactions, and sanctions.</li></ul>

#### **4. PREVENTIVE MEASURES – DESIGNATED NONFINANCIAL BUSINESSES AND PROFESSIONS**

##### **4.1. Customer Due Diligence and Record keeping (R.12)**

###### **4.1.1. Description and Analysis**

###### ***Legal Framework:***

872. The customer due diligence and record-keeping requirements for DNFBPs are set out in the AML Act. With minor variations (discussed below), these are the same for DNFBPs as those for financial institutions. The strengths and weaknesses of the general CDD and record-keeping regime are analyzed in Section 3 above and the comments there apply equally to DNFBPs.

873. The following is the list of German nonfinancial institutions that, under the AML Act, are subject to AML/CFT preventive measures (Section 2 numbers 7 to 12 of the Act):

874. “Lawyers, legal advisers who are members of a chamber of lawyers and registered persons as defined in Section 10 of the Legal Services Act, patent attorneys and notaries when they assist in the planning or execution of the following transactions for their clients:

- Buying and selling of real property or business entities;
- Managing of client money, securities or other assets;
- Opening or management of bank, savings or securities accounts;
- Procurement of funds required for the creation, operation or management of companies;
- Creation, operation or management of trusts, companies, or similar structures; or
- When they act on behalf of and for their client in any financial or real estate transaction.

875. Auditors, chartered accountants, tax advisers and tax agents.

876. Trust or company service providers not already covered under the previous two items when they provide the following services for third parties:

- a) Creating a legal person or partnership;
- b) Acting as a director or manager of a legal person or partnership, a partner of a partnership or a similar position;

- c) Providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement as defined in Section 1(6) second sentence no. 2;
- d) Acting as a trustee of a legal arrangement as defined in Section 1(6) second sentence no. 2;
- e) Acting as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements as defined in Section 2(5) of the Securities Trading Act in conformity with community legislation or subject to equivalent international standards; and
- f) Arranging for another person to act in the functions described under b, d, and e.
- Real estate agents;
  - Gambling casinos; and
  - Persons trading in goods.”

877. The obliged nonfinancial institutions under the AML Act encompass all the DNFBPs defined by the FATF. TCSP requirements generally fall under the obligations applicable to legal and accounting professionals, which typically are the providers of TCSP services. Office services, such as providing accommodation mailing addresses, and mail and answering services, which are provided by independent companies, are covered under general requirements for TCSP provisions of AML Act, but no arrangements have been made for compliance supervision. In some cases, the German specification of DNFBP activities that is covered by the AML Act is slightly broader than the FATF specification. The AML Act applies to accountants in all their activities and it also includes tax advisers in the category of accountants. Real estate agents are included without limitation to their involvement in transactions for their client concerning the buying and selling of real estate. All persons trading in goods are included, not just dealers in precious metals and precious stones.

878. The following table shows which categories of DNFBPs as defined by FATF are subject to AML/CFT obligations and the principal legislation regulating each of the professions and businesses:

**Statistical Table 25: DNFBPs and legislation regulating them**

Sector	Governing Law for AML/CFT	Regulatory Law
Casinos	AML Act	Gambling Treaty 2008; various individual <i>Länder</i> casino acts
Real Estate Agents	AML Act	Trade Law
Dealers in Precious Metals	AML Act	Trade Law and various individual <i>Länder</i> legislation
Dealers in Precious Stones	AML Act	Trade Law and various individual <i>Länder</i> legislation
Lawyers	AML Act	Federal Statute on Lawyers; Federal Statute on Patent Attorneys
Notaries	AML Act	Federal Statute on Notaries
Registered legal advisers	AML Act	Legal Services Act
Accountants	AML Act	Federal Statute on Auditors; Tax Consulting Act



Sector	Governing Law for AML/CFT	Regulatory Law
Trust and Company Service Providers	AML Act	Most TCSP services covered indirectly through application of AML Act to lawyers, notaries, independent legal professionals, and accountants. Office services are covered but not supervised for compliance.

879. The risk-based measures introduced in the AML Act and discussed in Section 3 apply also to DNFBPs. Risk sensitivity depends on the type of contracting party, business relationship, product, or transaction. (AML Act, Section 2.4). Section 2.4 also provides: “The institutions and persons covered by this Act shall be able to demonstrate to the competent authorities mentioned in Section 16 (2) that the extent of the measures is appropriate in view of the risks of ML and TF.”

### Specific Scope of CDD for DNFBPs

880. Although, in principle, the covered DNFBPs are subject to the same CDD, record-keeping, and monitoring obligations as financial institutions, the AML Act exempts some DNFBPs from some of the specific requirements. For casinos and dealers in precious metals and precious stones, the effect of the exemptions is to bring the scope of required due diligence into alignment with the scope expected under the FATF Recommendations.

881. The AML Act applies to persons (legal and natural) trading in goods; dealers in precious metals and precious stones are specific cases of persons trading in goods. Exceptions introduced in Section 3(2) have the effect of narrowing the CDD obligation for persons trading in goods to those cases in which cash payment is accepted in amounts of EUR 15 000 (USD 20 876) or more – apart from cases where there is reason to suspect that a transaction may have served or would serve the purpose of an offense pursuant to Section 261 of the CC (*Strafgesetzbuch*, StGB) or of TF (Section 3(2), third sentence, of the Money Laundering Act). This conforms to criteria c. 12.1.c in the Methodology.

882. The CDD obligation of gambling casinos is addressed specifically in Section 3(3) of the Act which provides that casinos “shall be required to verify the identity of customers buying or exchanging gambling chips with a value of EUR 2 000 (USD 2 783) or more. This requirement may also be met by verifying the identity of customers when they enter the gambling casino.” The EUR 2 000 threshold for identification is well within the limit established in c. 12.1.a.

883. Another (narrow) exemption to the generally applicable CDD requirements applies to those DNFBPs that provide legal advice. Under Section 3(6) of the AML Act, there is a general requirement that, if persons covered by the Act are unable to fulfill the CDD requirements, they may not establish or continue the business relationship or carry out transactions. Further, if a business relationship already exists, the institution or person covered by the Act shall terminate the relationship regardless of other legal or contractual provisions. These general provisions of the Act address the requirements under c.5.15 and 5.16. As an exception to this general provision, Section 3(6) provides that the obligation to not establish or continue a relationship does not apply “when the contracting party seeks legal advice or representation in proceedings unless the institution or person concerned *knows* that the contracting party is utilizing the legal advice for the purpose of ML or TF.” This exemption for legal advice is based on the principle that all persons are entitled to legal advice and representation in legal proceedings. As analyzed in more detail below, legal advice is interpreted quite broadly in Germany and the exemption from certain CDD requirements because of legal advice appears to be more expansive than contemplated in the Methodology.

***CDD Measures for DNFBPs in Set Circumstances (Applying c. 5.1-5.18 in R. 5 to DNFBP) (c. 12.1):***

884. Other than the exemptions noted above, under the AML Act, the CDD requirements covered by c.5.1-5.18 are the same for DNFBPs as those for financial institutions. See the discussion and analysis of r.5 above for an analysis of the extent to which these legal requirements do or do not comply with Recommendation 5. The following material further analyzes the specific exemptions applicable to DNFBPs, discusses how the requirements are applied in the different DNFBP sectors, and evaluates the effectiveness of implementation of Recommendation 5 by the various DNFBP sectors.

**Casinos**

885. *Internet Casinos.* Regulation of casinos is governed by *Länder* legislation, not federal legislation. In order to harmonize some elements of gambling legislation across *Länder*, particularly the social and consumer protection aspects of gambling, and to satisfy various court rulings, the 16 *Länder* governments entered into a treaty, the State Gambling Treaty, which came into effect on January 1, 2008. The provisions of the Treaty have all been incorporated into the laws of the 16 *Länder*. Some sections of the Treaty deal with casinos. Among other things, the Treaty prohibits internet casinos. According to paragraph (4) of Section 4 (General Provisions) of the Treaty, “The organizing and arranging of public games of chance on the Internet is prohibited.” Casino operators confirm that they have closed down the internet gambling services they offered before the Treaty came into effect. The prohibition of internet gambling in the State Gambling Treaty is reinforced by provisions of the German CC. Offering internet casinos is a prohibited organization of public games of chance (Section 284 of the CC, the use of such internet gambling services is participation in prohibited public games of chance (Section 285 of the CC). Both offenses are prohibited by threat of punishment and are applicable regardless of whether the casino operator has his seat of company within the country or abroad. Relevant only is the access to such internet gambling services within the German territory.

886. *Land-Based Casinos.* In accordance with the AML Act, all casino customers are identified when they enter the casino. Basic details are recorded, including passport number or similar identification number. Some casinos have electronic readers capable of scanning and recording German identity cards and passports. In addition, in order to facilitate entry as well as casino services, frequent visitors are encouraged to apply for a casino card that records all basic identity information on a machine readable card. It is common practice to re-swipe the identity card on departure from the casino or to otherwise note the time guests leave.

887. Within Germany, casinos have long had arrangements for exchanging information among themselves about undesirable patrons who have been barred from playing in any casino. The primary focus of this arrangement has been consumer protection to reduce gambling addiction but the information exchanged extends to undesirable patrons generally. This information is now available on an online database and, at entry, visitor names are cross checked with the database allowing the casino to identify riskier clients and bar them from entry. The arrangements for barring individuals from entering casinos has been explicitly recognized under the 2008 State Gambling Treaty database which also extended the scope of the database to include individuals barred from state lotteries, including those who may be barred because of unsuitability, such as gambling addiction. The barring arrangements have been interpreted as being consistent with European privacy and data protection laws since casino operations are illegal unless specifically authorized. The database does not include information on customers who may have been barred in other countries.

888. Under the AML Act the threshold at which identification of customers is required is transactions of EUR 2 000 (USD 2 783) or more, well within the USD or EUR 3 000 called for under Recommendation 12(c 12.1.a). Standard casino practice is to take advantage of the provision in the Act

that allows this identification requirement to be met by identifying customers on entry. Under routine circumstances, no further identity checks takes place on purchase or cash-out of chips or on cash-out of slot machine winnings. Nevertheless, a close observation following a higher purchase of chips is a common practice and some casinos carry out further identity check and make notes in case of higher amounts of money being changed. German casinos generally operate on a cash-in, cash-out basis. Only Euros are used; foreign currency is not accepted. Operators state that it is very exceptional for German casinos to provide currency exchange facilities at the cage because the expense of providing such facilities cannot be justified. Casinos do not provide house credit but credit cards are accepted. Large or unusual credit card purchases would trigger additional scrutiny, primarily for credit risk purposes, but this may entail additional identity verification. Casino practices under the identify-on-entry arrangements fall short of the requirements of Recommendation 12 in that the arrangements do not generally ensure that casinos are able to link customer due diligence information for a particular customer to the transactions that the customer conducts in the casino (c. 12.1.a, footnote 21).

889. For security reasons, large payouts may be made by check, which may entail additional verification of identity. Casinos do not issue a winnings receipt and casino operators state that the checks issued do not provide any statement indicating that the check represents winnings. This is taken to mean that a bank accepting deposit of the casino check would not be able to use the check as evidence that the funds had come from gambling winnings. In very exceptional circumstances, arrangements may be made to have winnings wire transferred to a customer's bank account, but such transfers are subject to full documentation, including additional verification of customer information. Operators state that, in general, the popularity of German casinos has been in decline and high rollers are now uncommon and that average client net expenditures are now under EUR 150 (USD 209). No national statistics were available on the extent to which payouts are made by check or by wire transfer to a customer account.

890. Casino operators generally were of the view that because they operated primarily on a cash-in, cash-out basis, the risks of ML in German casinos were relatively low. In addition, German casinos do not cater to more vulnerable clients such as high rollers and casino tourism. Also, the German criminal provision prohibiting casinos unless formally licensed applies to German high-seas cruise ships, since they qualify as German territory (Section 4 of the CC). While the structure of the German casino industry may mitigate significant potential vulnerabilities, operators did not appear to be alert to many of the complex and sophisticated arrangements for using casinos to launder money, such as those discussed in the March 2009 FATF Report "Vulnerabilities of Casinos and Gaming Sector." While some transactions and some customers may trigger some enhanced due diligence, no systematic risk rating procedures have been developed to recognize and identify clients that pose a high ML risk.

### **Real Estate Agents**

891. Under Section 34c, (1), no. 1 of the German Trade Regulations Act (GewO), real estate agents are subject to business licensing requirements before they undertake work in the field of professionally brokering contracts which involve real property, rights equivalent to real property, commercial space or residential space or documenting in the ordinary course of business, contract-making opportunities. The GewO is administered by trade supervisory offices at the *Länder* level, typically under the authority of the regional Ministry of Economy or, for some purposes, under a regional court. The Act provides that a business license shall be withheld if there are grounds to indicate that the applicant or management is not reliable enough to conduct business or the applicant is in a precarious financial situation. The Act expressly provides that a person shall be deemed to lack the necessary reliability if he has been convicted in the last five years before application of a crime or of theft, embezzlement, extortion, fraud, breach of trust, ML, falsification of a document, receiving stolen goods, profiteering, or criminal insolvency.

892. In Germany, all real estate transactions are required to be notarized and all escrow arrangements are handled by a notary. Real estate agents do not receive or hold client's funds. The real estate agent participates in the transaction in the role of bringing together a buyer and seller and mediating a provisional understanding on basic terms of an agreement. A formal contract, however, is only executed under the agency of a notary. For real estate agents, dual agency is the rule, with the real estate agent representing both the buyer and seller. Exclusive listings for fixed periods are exceptional. Sellers may list their property with multiple agents.

893. These features of the real estate market limit the extent to which a real estate agent, in the normal course of business, undertakes due diligence on clients. While a listing agreement appears to constitute "establishing a business relationship" as well as meeting the test of carrying out an occasional transaction above the threshold of EUR 15 000 (USD 20 876), lack of exclusivity limits the incentive of the agent to fully identify client at the beginning of an engagement. Lack of exclusive listings apparently leads to frequent disputes about whether a commission is or is not owed. To avoid paying a commission, it is not uncommon for different, but affiliated, buyers or sellers, other than those the agent has dealt with, to meet with the notary to conclude a contract. The potential for straw man transactions undermines the value of CDD carried out by real estate agents prior to the conclusion of a contract. The requirement for a notary to be involved, likewise, limits the incentive of a real estate agent to identify clients since a contract will not be firm until executed through the notary, who has responsibility for complete due diligence on the parties to the contract. These structural features notwithstanding, the real estate agent will need to gather sufficient information to represent the suitability and capacity of a buyer to a seller, as well as to establish the seller's ownership interest in a property.

894. Real estate agents who met with assessors were aware that they were subject to the provisions of the AML Act. They generally considered that since they did not accept client funds and since both notaries and banks would be involved in any transactions, they would not be expected to undertake regular due diligence on clients. Also, because they do not accept client funds, they considered that they were unlikely to be involved in a transaction involving ML. As described by the real estate agents, their current practices fall short of the FATF standards which require CDD "when they are involved in transactions for their client concerning the buying and selling of real estate" without regard to whether client funds are handled or whether other parties are involved in the transaction.

895. Regional authorities with responsibility for administering laws applicable to real estate agents have not issued any guidelines with respect to how real estate agents should comply with the AML Act, nor have they undertaken any awareness-raising campaigns with the sector. Approximately half of the 12 000 agents in Germany are members of a national association of real estate agents. The association has sent statements to its members notifying them that they are subject to the 2008 AML Act and informing them that AML information is available on the website of the FIU. The association did not believe that any general information or typologies had been published on the ML and TF vulnerabilities of the real estate sector, other than some brief, general information on the FIU website. Nor were they aware of any risk rating systems that might have been adopted by any real estate agent.

### **Dealers in Precious Metals and Dealers in Precious Stones**

896. Germany has taken the approach of including all "persons trading in goods" within the scope of the preventive measures obligations under the AML Act. This includes, but is not limited to, dealers in precious metals and dealers in precious stones. Under Section 3(2) of the Act, persons trading in goods are required to carry out due diligence "only when accepting cash amounting to EUR 15 000 (USD 20 876) or more," "whether the transaction is carried out in a single operation or in several operations totaling EUR 15 000 or more."

897. As is the case with real estate agents, dealers in precious metals and dealers in precious stones are not specifically regulated professions. However, their activities do come under the Trade Law. Administration of the Trade Law is the exclusive responsibility of the 16 *Länder*; the federal government cannot regulate supervisory competencies in the area of trade legislation. Administration of trade legislation typically comes under the authority of the *Länder* Ministry of Economy and is carried out through district or municipal offices.

898. Almost no information was available to the mission on the general practices of dealers in precious metals and dealers in precious stones with respect to compliance with their obligations under the AML Act. At least two associations represent the sectors: (a) Federation of German Jewelry, Watches & Clocks, Silverware and Related Industries, and (b) Federal Association of the Precious Stones and Diamond Industry. However, these associations are headquartered in southwest Germany and were not available to meet with the mission. Nor did contacts with *Länder* Ministries in Hesse and Berlin identify any officials knowledgeable about the precious metals and precious stones businesses. More generally, *Länder* officials were not aware of any steps being taken to ensure compliance by any “persons trading in goods” with their CDD obligations under the AML Act.

### **Legal professions**

899. The structure of the formal AML/CFT obligations for lawyers, legal advisers who are members of a chamber of lawyers and registered persons as defined in Section 10 of the Legal Services Act, and patent attorneys (collectively, the legal professions), is identical across all categories. This structure is slightly different than that for other DNFBPs in that the scope of lawyers’ activities subject to preventive measures is limited. Thus, under Section 2(7) of the AML Act, the due diligence obligations arise “when they assist in the planning or execution of the following transactions for their clients:

- a) Buying and selling of real property or business entities,
- b) Managing of client money, securities or other assets,
- c) Opening or management of bank, savings or securities accounts,
- d) Procurement of funds required for the creation, operation or management of companies,
- e) Creation, operation or management of trusts, companies or similar structures, or
- f) When they act on behalf of and for their client in any financial or real estate transaction.”

900. This specification of scope includes all the situations specified in Recommendation 12.

901. Section 3 (1) of the Act spells out the general due diligence that all covered parties are to carry out, including the legal professions. It addresses all the criteria of Recommendation 5. (See the discussion and analysis under Recommendation 5 above for a complete analysis of these sections of the legal framework and their compliance with the FATF standards).

902. *Note on legal professional privilege.* While legal professional privilege is addressed in the methodology and in this assessment under R. 16, it also has a bearing on compliance with R. 12. As noted above, under Section 3(6) of the AML Act, there is a carve-out from the general requirement to terminate a relationship in cases where CDD cannot be completed “when the contracting party seeks legal advising or representation in proceedings.” As implemented in Germany, exemptions or carve-outs for “legal advising” or legal or professional privilege are applied quite broadly and appear to go beyond the norms of



national discretion contemplated in the FATF Interpretative Note 16 (IN 16). Per this IN, “it is for each jurisdiction to determine the matters that would fall under legal professional privilege or professional secrecy.” Further, such legal privilege would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings. The language of the exemption under Section 3(6) for situations of “legal advising” is broader than the “ascertaining of the legal position of their client” language of Interpretative Note 16. In line with IN 16, legal professional privilege extends beyond legal professionals (lawyers, patent lawyers, notaries and registered legal advisors) and includes the accounting professions (auditors, chartered accountants, and tax advisers).

903. While inclusion of the accounting profession is contemplated under IN 16, the auditors, chartered accountants, and tax advisers who met with assessors appeared to take an expansive view of what is covered by such privilege, stating that much of their professional work is included since it involved advising clients on how to satisfy their legal obligations. Legal professionals took a more nuanced but also relatively broad view of what matters would be covered by legal advising. No general guidance has been provided regarding what matters are or are not included within the scope of the carve-out for “legal advising.”

904. Beyond the provisions of the AML Act, lawyers, patent attorneys, notaries, auditors, accountants, and tax advisers are all subject to strict professional secrecy obligations. (Legal advisers registered by local courts are not subject to statutory professional secrecy obligations.) Under the CC, violations of professional secrecy are subject to criminal sanctions. Customer identification information is understood to be covered by professional secrecy. In keeping with this, the relevant professions will only provide CDD details to another party if the client specifically authorizes release of such information. A court order is required for a law enforcement investigator to obtain CDD information from a member of the relevant professions. Also, the relevant professions are not permitted to give testimony in a legal proceeding about any client information that is subject to professional secrecy provisions, including CDD information.

905. As implemented, aspects of legal professional secrecy provisions undercut full compliance with R. 12 in two respects: (a) the overly broad interpretation of the scope of “legal advising” allows a broad exemption from the requirements of c 5.15 and 5.16 with respect to terminating a relationship when full CDD cannot be completed, and (b) restrictions on release of CDD data inhibit compliance with c. 10.3 which calls for all customer and transactions records and information to be available on a timely basis to domestic competent authorities upon appropriate authorities.

## Lawyers

906. While lawyers are not precluded from the activities spelled out in Recommendation 12, German lawyers are only engaged to a limited extent in the activities that make them subject to the preventive measures sections of the AML Act. Contracts covering purchase and sales of real property and business entities all require notarization so the execution of these transactions is handled almost exclusively by notaries, although lawyers may have some involvement in advising and planning of the transactions. Managing of client money, securities or other assets also is handled most frequently by banks or by notaries, who frequently provide an escrow function in the buying and selling of assets. Lawyers do maintain lawyers trust accounts at banks. Under Section 4 (2) of the Lawyers Rules of Professional Practice, client funds are to be passed on immediately; when that is not possible, they should normally be held in a separate account on behalf of one individual client, where the name of the client is identified to the bank by the lawyer. Amounts held in a collective clients’ account cannot exceed EUR 15 000 (USD 20 876) and are not to be held for more than one month. Opening or managing of bank, savings, or securities accounts are also not customary services of German lawyers.



907. Under the Federal Lawyers Act, responsibility for the management and oversight of lawyers rests with regional Chambers of Lawyers. The Federal Chamber of Lawyers is an umbrella organization representing all of the regional chambers. Outreach with respect to AML obligations has been one activity of the chambers. The Federal Chamber has provided information notices to the regional chambers, and through them, to their members informing them of their responsibilities under the 2008 AML Act. In addition, Federal Chamber newsletters, magazine articles, and speeches have discussed and provided explanations of various aspects of lawyers' CDD obligations under the Act. Also, discussion of AML preventive measures has been an agenda item in semi-annual membership meetings of regional chambers. To a limited extent, the Federal Chamber has provided training sessions for law firms, usually by request and mainly for larger law firms. No specific guidance has been issued by the Federal Chamber with respect to AML/CFT compliance by lawyers but a paper is being prepared. Guidance applicable to all professional groups, not just to lawyers, has been issued by other official bodies. In 2004, a study jointly commissioned by the Federal Ministry of Justice and the Federal Ministry of the Interior entitled "Money Laundering Vulnerability of Lawyers, Tax Advisors, Notaries and Auditors" was published by the Max Planck Institute for Foreign and International Criminal Law. Also, in October 2003, the FIU, in collaboration with several associations and regional governments, published guidance on "Possible money laundering indications in accordance with Section 261 of the CC relevant to newly-obliged parties, for professional groups pursuant to Section 3(1) numbers 1 and 2 of the Money Laundering Act."

908. While the regional chambers have SRO authority to oversee the AML/CFT compliance of lawyers, they do not have authority to do routine examination of files to monitor compliance. Hence, no direct independent evidence is available on the extent to which lawyers effectively implement their due diligence obligations under the AML Act. Chamber officials note that in cases where investigations of lawyers have been undertaken because of complaints or for other reasons, these investigations have not generally revealed problems with AML compliance. They also considered that due diligence is a customary part of a lawyer's practice so the specific requirements under the AML Act are familiar to lawyers.

909. In discussions with chamber officials and with practicing lawyers, the view was frequently expressed that the profession was low risk with respect to ML or the financing of terrorism. This view was typically justified on the basis that the legal profession is strictly regulated and that normal client acceptance procedures would weed out risky clients in the activities covered by AML obligations. Further, it was frequently stated that lawyers had limited vulnerability to involvement in ML since they typically do not handle client funds. In the assessors view, the overly facile assumption that the legal profession is low risk suggests a limited awareness of the variety of vulnerabilities of the legal profession to misuse by money launderers and a need for additional training.

### **Patent Attorneys**

910. The legal framework for AML/CFT due diligence requirements for patent attorneys is identical to that for other lawyers. Patent attorneys have specialized expertise in science and technology and are qualified lawyers in the area of intellectual property law. They are qualified to represent clients before the German Patent Office and the German Patent Court, or on appeal or in matters involving technical issues, in higher courts. Because their legal expertise is highly specialized, they are organized under their own Chamber, the Chamber of Patent Attorneys, and are not generally qualified to advise or represent clients outside of their area of legal expertise.

911. Because of their specialization, patent attorneys do not typically become involved in most of the activities listed in Recommendation 12 that bring lawyers within the scope of the FATF Recommendations, such as buying and selling real estate, management of client funds, management of financial accounts, etc. Patent attorneys do advise and participate in negotiation and contracting for the

purchase and sale of intellectual property rights. While, for tax planning purposes, it is not uncommon for intellectual property rights to be lodged in special purpose vehicles, including in offshore centers, representatives of the Chamber of Patent Attorneys state that they are not aware of German patent attorneys being involved in making such arrangements or becoming involved in negotiating such matters as transfer prices. As a business matter, others are better qualified in such transactions and patent attorneys are more valuably employed in their area of specialization. Patent attorneys typically work with a well established, stable list of clients, many of which are listed companies. It is generally accepted in Germany that patent attorneys have a low vulnerability to ML or TF and Chamber representatives were not aware of any typologies linking intellectual property transactions to ML.

912. Based on discussions with the Chamber, patent attorneys are aware that they have obligations under the AML Act, but specific compliance measures have not been adopted by patent attorneys, in part because the likelihood of being involved in transactions within the scope of law is considered to be remote. The Chamber has formal responsibility for oversight of AML/CFT compliance of its members. The Chamber does not have authority to undertake routine compliance examinations, but it can review compliance in the context of an investigation of a member initiated for some other reason. To date, it has not had any reason to do so.

### **Notaries**

913. Of the legal professions, notaries are the parties most involved in the transactions itemized in Recommendation 12, item d. Notaries play an official function in advising and attesting to the legal validity of contracts and carrying out legally required due diligence on the contracting parties. Contracts for the purchase and sale of real estate and of companies are required to be notarized. This can include advice on the suitability as well as the legality of proposed terms. However, notaries represent both sides of a contract in a disinterested manner and do not become involved in providing tactical or strategic advice on how a transaction should be structured. Similarly, notaries are not generally involved in the procurement of funds for companies or the creation, operation or management of trusts companies or other similar structures. Notaries play an escrow role in completing purchase and sale of property and commonly hold client funds and securities pending settlement, including holding client funds in notaries trust accounts at banks.

914. Due to the nature of their core function, notaries have well established procedures and considerable experience in carrying out the due diligence called for under the FATF Recommendations and required under the AML Act. Representatives of the Chamber of Notaries and practicing notaries demonstrated a thorough understanding of their obligations under the AML Act and how these obligations fit into their overall functions.

### **Legal Advisers who are members of chamber of lawyers**

915. The AML Act includes legal advisers who are members of chamber of lawyers as covered parties. Until 1980, legal advisers were recognized under the 1935 Legal Consultancy Act but did not have the opportunity to be a member of a chamber of lawyers. In 1980, the profession was closed and no new legal advisers were admitted. However, anyone who had been admitted to practice as a legal adviser up until 1980 was given the opportunity to become a member of a chamber of lawyers. With the passage of time, very few remain active today. These legal advisers have the same AML/CFT obligations as fully-qualified lawyers and are under the supervision of the Chamber of Lawyers, including for AML/CFT compliance.

## **Registered persons as defined in Section 10 of the Legal Services Act**

916. The AML Act includes as covered parties registered persons as defined in Section 10 of the 2007 Legal Services Act. The Legal Service Act (LSA), which has been enforced since July 2008, replaced the 1935 Legal Consultancy Act. The purpose of the LSA is to regulate the provision of out of court legal advice by parties that are not members of chambers, with a view to partially liberalizing such activity while protecting the public from unqualified legal advisers. Registration is not required if the legal advice offered is part and parcel of the activity of another profession (*e.g.* an architect or engineer). However, the LSA does require (as did the earlier Legal Consultancy Act) registration of persons who provide legal advice with respect to three specific lines of business: (a) debt collection services, (b) pension consultancy, and (c) consultancy on foreign law. Registration is administered by a regional court. The registering court is also the supervisor for compliance.

917. While the FATF glossary does not give a definition of legal professionals, registered persons under the LSA fit into a reasonable interpretation of this profession. Inclusion as a registered person is based on the party being a professional offering legal advice. Consultancy on foreign law requires expertise in foreign law as a condition of registration. Registered persons are not precluded from carrying out for clients any of the activities listed in criteria 12.1d.

918. Application of an AML compliance regime for registered legal advisers is relatively new. Experience has not yet developed as to the extent to which the registered legal advisers are familiar with their CDD obligations, or have developed operational compliance practices. Nor have oversight practices been developed, although the Act provides legal authority for oversight.

919. Although registered legal advisers have a contractual obligation to maintain confidentiality in their professional dealings, they are not subject to the same strict statutory professional secrecy obligations that apply to other legal professions. Nevertheless, the AML Act extends the same exemptions to registered legal advisers that it extends to the professions subject to professional secrecy obligations.

## **Accounting Professions**

920. The CDD legal framework for the accounting professions (auditors, chartered accountants, tax advisers, and tax agents) is identical to the framework for lawyers discussed above. The only significant difference is the scope of application of the AML/CFT obligations. All activities of the accounting professions are subject to the AML Act, rather than just the enumerated activities applicable for lawyers. The analysis of the CDD legal framework above and under Recommendation 5 of this report is equally applicable to the accounting professions.

## **Auditors**

921. As the SRO for auditors, the Chamber of Auditors has responsibility for members' compliance with their obligations under the AML Act. In this capacity, it has circulated to the profession notice of their obligations under the 2008 Act, including comments on how these requirements apply specifically to auditors. In May 2009, the Institute issued guidance on implementation of AML/CFT preventive measures under the AML Act. Among other things, the guidelines, which are advisory only, elaborate on many of the details of how to comply with the due diligence required under the Act. Also the requirements for a risk-based approach are discussed. Training on the Act for members of chambers is being planned for later this year.

922. The Institute of the Chamber of Auditors (a private special interest group of auditors and auditing firms that also carries out academic surveys and studies and offers vocational training for auditors) is

researching the ML and TF vulnerabilities of the auditing profession but has not yet issued any reports. Some auditors expressed a view that auditing is likely to be a low-risk activity because money launderers would try to avoid involvement in entities that are subject to statutory audits.

923. In recent years, the Chambers of Auditors has developed and extended quality assurance programs designed to test whether auditors are fulfilling their professional obligations and to evaluate the quality of their work. Although the focus of the quality assurance work is auditing, the program allows for on-site visits and can include compliance with due diligence requirements. Chamber members stated that no CDD compliance issues have emerged from these reviews.

### **Tax Advisers**

924. The regional chambers are the SROs for their members. In this SRO capacity, the chambers have issued notices to members advising them of their obligations under the AML Act. In April 2009, the Federal Chamber published guidance on how the AML Act requirements could be implemented by tax advisers. Additionally, the Federal Chamber has posted on its website a variety of references such as the third EU directive, guidance, notices and typologies issued by the FIU, and notices about new methods of ML. No systematic review has been conducted of the ML vulnerabilities of the sector.

925. Chambers of Tax Advisers do not have authority to do routine, on-site, compliance examinations, so there has been no systematic, independent review of tax advisers' compliance with their CDD obligations. In discussions, members of Chambers of Auditors were fully familiar with the CDD obligations of tax advisers under the Act. They were not, however, in a position to comment on how well these requirements are being implemented across their widely disbursed membership.

### **Tax agents**

926. The AML Act (Section 2 (8)) includes tax agents as a profession covered under the Act. Tax agents are a discontinued category of tax adviser. Tax agents, to the extent they still practice under that title, have all been absorbed into the Chamber of Tax Advisers and are subject to the same obligations and disciplinary rules as all tax advisers.

### **Trust and Company Service Providers**

927. The AML Act (Section 2(9)) applies to trust and company services providers if they are not already covered under one of the legal professions or one of the accounting professions, when they provide specific services. The list of specific services covers the services set out in Recommendation 12. In Germany, it is understood that the listed services are typically provided by the legal or accounting professions or by banks. The authorities have not identified any other group of persons that offers these services as a regular part of their business.

### ***CDD Measures for DNFBPs in Set Circumstances (Applying Criteria under R. 6 & 8-11 to DNFBP) (c.12.2):***

928. R 6. – PEPs – The obligations of DNFBPs with respect to PEPs are the same as those for financial institutions. The discussion of the adequacy of these requirements in Section 3 above is equally applicable to DNFBPs. The following material discusses the effectiveness of implementation of these requirements by PEPs.

929. c.6.1. No specific requirements have been imposed on any DNFBPs to put in place appropriate risk management systems to determine whether a potential customer, a customer, or the beneficial owner is

a PEP. Under the AML Act, DNFBPs, unlike financial institutions, are exempted from the requirement to have a compliance officer. In addition, instructions issued by the Chamber of Lawyers, the Chamber of Notaries, the Chamber of Auditors, and the Chamber of Tax Advisers, under authority in the AML Act, have exempted member firms with 10 or fewer professionals from compliance with other safeguard measures enumerated in Section 9 of the Act. This exemption includes exemption from the requirement for “developing and updating internal principles, appropriate business and customer-related safeguards and controls to prevent ML and TF.” As an operational matter only the very largest law firms, notaries and accounting firms appear to subscribe to data services providing information on PEPs.

930. c.6.2-6.4. No specific requirements have been imposed on DNFBPs to obtain senior management approval for establishing business relationships with a PEP. The relevant PEP approval requirements are those set out in Section 6(2)(a) of the AML Act which calls for consent of the immediate supervisor of next management level when establishing a business relationship through an intermediary. Criteria 6.2 calls for approval by senior management, not just by a supervisor or next level of management, for all business relationships with a PEP, not just those established via intermediaries. In large law firms and accounting firms, client acceptance policies and procedures typically call for senior management approval for establishing business relationships with a PEP. Smaller practices do not appear to have such arrangements.

*c. 6.5-c.6.6. Refer to section 3 above.*

#### ***R. 8 Non-face-to-face transactions; new technologies.***

931. c.8.1-c8.3. No requirements with respect to non-face-to-face transactions and new technologies beyond the requirements set out in the AML Act.

#### ***R. 9 Intermediaries/Introduced business.***

932. c.9-1c.9.5. The procedures for DNFBPs for dealing with intermediaries and introduced business are those authorized under the AML Act. The analysis in Section 3 is relevant with respect to the provisions of the Act. In general, German covered professions appear to rely on the published lists of equivalent jurisdictions to evaluate whether a professional counterpart in another jurisdiction is adequately supervised for AML/CFT and can be relied on to carry out CDD. If so, additional CDD on the counterpart is not done.

#### ***R. 10 Recordkeeping***

933. c. 10.1-c.10.3 The AML Act requires that due diligence data and information gathered on contracting parties, economic beneficiaries, business relationships and transactions are recorded and that records be retained for five years. It also imposes some standards on the format and retrievability of such records. See the analysis in Section 3 above for an analysis of the adequacy of these requirements in terms of R. 10. In addition to requirements of the AML Act, the various laws regulating the professions generally include record-keeping requirements similar or more detailed to those in the AML Act. C 10.3 calls for (FIs) regulated parties to be “required to ensure that all customer and transaction records and information to be available on a timely basis to domestic competent authorities upon appropriate authority. As discussed above, under the professional secrecy regime applied to lawyers, independent legal professionals, notaries, and accounting professionals, customer and transaction records and information are only provided to competent authorities under strict conditions.

934. c. 10.1.1 sets out a requirement that “transactions records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal.” While the professions may be able to maintain records in the appropriate detail, they are unlikely



to be allowed to be used in criminal proceedings because of professional secrecy obligations. (See below for further analysis of professional secrecy obligations.)

### ***R. 11 Monitoring (applying c.11.1, c.11.2, and c.11.3 to DNFBPs)***

935. c. 11.1 and c. 11.2 The requirements under the AML Act to pay attention to all complex, unusual large transactions, etc. are the same for DNFBPs as they are for all financial institutions. For an analysis of the adequacy of these requirements, refer to the discussion and analysis under R. 11.

936. c. 11.3. Under the AML Act, DNFBPs are subject to the same five-year record retention requirement as are all financial institutions. See the discussion and analysis under R. 11. As discussed more fully under R. 16, professional secrecy provisions pose significant impediments to the authorities' access to the records of the legal and accounting professions.

### ***Analysis of Effectiveness***

937. Implementation of CDD requirements across the DNFBP sectors is checkered. In the casino sector, identification practices fall well short of the criteria established in Recommendation 12.1 and monitoring for ML has significant weaknesses. No procedures appear to have been put in place to promote compliance by dealers in precious metals and precious stones (dealers in goods, more generally) with the identification requirements for cash transactions in excess of EUR 15 000 (USD 20 876). Based on discussions with industry representatives, real estate agents are aware that they are subject to the AML Act, but do not appear to be taking systematic steps to comply, in part, because the requirements do not fit within their customary business practices and, in part, because supervisory arrangements to promote compliance are underdeveloped. Among the legal and accounting professions, awareness and policies and procedures for CDD compliance are better developed, although the complexities of identification of beneficial ownership are not widely appreciated. Implementation appears to be strongest among notaries, in part, because aspects of CDD are a core element of the work of notaries, but also because of a proactive role by the Chamber of Notaries and independent supervision by the courts.

938. As discussed in more detail below, supervisors do not have authority to carry out routine examinations of AML/CFT compliance of lawyers and tax advisers so there has been no independent evaluation of the extent to which these professions are addressing their CDD obligations. Based on discussions with a cross section of the legal and accounting professions, there appears to be a common assumption that the ML and TF vulnerabilities of each of the sectors are low. Many comments suggested an inherent belief that, because the professions are well regulated and do not deal in cash, their clients and services are consequently relatively low risk. In part, this reflects a narrow perception of ML and TF risks that focuses mainly on the placement stage with less attention to the more sophisticated techniques that may be used to layer or integrate illegal proceeds into the legitimate economy. Few of the legal and accounting professionals interviewed had developed systematic procedures for identifying and monitoring the ML and TF risks of their clients or their services.

939. While DNFBPs are generally aware of their additional CDD obligations in set circumstances, additional safeguards do not appear to have been put in place to satisfy these obligations. With no risk management requirements to have procedures to identify PEPs, such identification does not appear to be a high priority for most DNFBPs. Also, the regulatory imperative to pay close attention to the requirements in set circumstances is dulled by the exemption of DNFBPs from the requirement to have a control officer, as well as the exemption of smaller firms from the requirement to adopt internal safeguards. DNFBPs are not generally subject to systematic oversight of CDD compliance, and, absent such monitoring, it is difficult to evaluate the extent to which they do or do not comply with their obligations with respect to Recommendations 6 and 8-11.



#### 4.1.2. Recommendations and Comments

940. In order to comply fully with Recommendation 12, Germany should do the following:

- Casinos should be required to adopt policies and procedures to link individual transactions to identified clients.
- DNFBPs should be required to have procedures for identifying PEPs.
- The recommended actions in Section 3 above with respect to R 5, 6, 9-11 should be implemented for DNFBPs, including, in particular, the need for a requirement to consider filing an STR in case of failure to complete CDD and for verification of beneficial ownership in all cases.
- Registered legal advisers, who are not subject to the same statutory professional secrecy obligations as the other liberal professions, should be excluded from the carve-out for legal and professional privilege.
- For full compliance with the Recommendations, the carve-out for legal and professional secrecy should generally be limited to information (a) obtained in the course of ascertaining the legal position of a client, or (b) in performing their task of defending or representing that client in or concerning judicial, administrative, arbitration, or mediation proceedings.
- Implementation
  - Arrangements should be put in place to monitor and ensure CDD compliance by TCSPs; and routine CDD compliance monitoring should be strengthened by the authorities responsible for overseeing compliance by real estate agents, dealers in precious metals and dealers in precious stones, lawyers, auditors, accountants, and tax advisors.
  - Outreach and Awareness raising
    - The authorities should develop outreach campaigns specifically to raise awareness of CDD obligations of real estate agents and dealers in precious metals and precious stones and, more generally to raise awareness of ML and TF risks in all of the DNFBP sectors.
  - Training
    - Casino staff and managers should be given additional training in ML techniques and risks.
    - CDD training requirements for real estate agents and dealers in precious metals and dealers in precious stones should be implemented
    - CDD training programs for lawyers, notaries, and auditors should be intensified.

#### 4.1.3. Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
R.12	NC	<ul style="list-style-type: none"> <li>• No arrangements for casinos to link identification-on-entry data to individual transactions within the casino.</li> <li>• Low awareness of CDD obligations and ML vulnerability among real estate agents and no oversight of compliance with CDD obligations of real estate</li> </ul>

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
		<p>agents and dealers in precious metals and precious stones.</p> <ul style="list-style-type: none"> <li>• No arrangements to promote and ensure AML/CFT compliance by TCSPs.</li> <li>• Inadequate awareness of ML and TF risks by casino operators, real estate agents, lawyers, notaries and auditors; underdeveloped risk assessment procedures.</li> <li>• Registered legal advisers are not subject to professional secrecy, they should not be included in the carve-out for legal and professional privilege.</li> <li>• No requirements for procedures to identify PEPs, or to consider filing an STR in cases where CDD cannot be completed, or to establish beneficial ownership in all cases.</li> <li>• Professional secrecy provisions are interpreted broadly by the liberal professions, and pose a significant impediment to their ability to provide records as evidence for prosecution of a crime (as called for under c 10.1.1) or keep findings available for competent authorities (as called for under c. 11.3).</li> </ul>

## 4.2. Suspicious Transaction Reporting (R.16)

### 4.2.1. Description and Analysis

#### *Legal Framework:*

941. The requirement for covered persons to file STRs is set out in Section 11 of the AML Act. The legal framework of the general requirements of Section 11 and the day-to-day operation of the reporting regime are analyzed in Sections 1, 2, and 3 above. The analysis there is equally applicable to DNFBPs. There are two significant differences between the general reporting framework applicable to financial institutions and that applicable to some of the DNFBPs. Section 11(3) of the Act provides a carve-out for legal privilege and professional secrecy; and Section 11(3) allows for members of professional chambers to transmit their STRs to their competent federal chambers.

942. Under Section 11(3), those persons covered by the carve-out “are not obliged to make a report if their suspicion is based on information from or about their client obtained while providing legal advice or legal representation in court for this client.” This exemption is subject to the condition that “The obligation shall remain in effect if the persons referred to in the first sentence know that their client is deliberately using their legal advice for the purpose of ML or TF.” The scope of the exemption — for legal advice and representation in court proceedings, as well as the condition for the exception to the exemption — go beyond the norms provided for in Interpretative Note 16, as discussed in the *note on legal privilege* in the discussion of R.12 above.

943. Interpretive Note 16 also provides that the exemption would normally apply to privileged information received by lawyers, notaries, or other legal professionals. It also provides for accountants to be exempted from reporting, where they are subject to the same obligations of secrecy or privilege. The German exemption covers both groups. Under Section 11(3) of the Act, lawyers, legal advisers who are members of a chamber of lawyers, and registered persons as defined in Section 10 of the Legal Services

Act<sup>71</sup>, patent attorneys and notaries are under the carve-out for legal privilege and professional secrecy. The same section also extends the carve-out to auditors, chartered accountants, tax advisers, and tax agents.

944. The legislation regulating the professions of lawyers, patent lawyers, and notaries, and the professional codes of conduct issued under authority of regulatory acts, contain language requiring professional secrecy. Under Section 43a of the Federal Lawyers' Code, which covers the Basic Duties of a Lawyer, paragraph 2 states: "A lawyer has a duty to observe professional secrecy. This duty relates to everything that becomes known to [the lawyer] in the course of the practice of [the] profession. This does not apply to facts that are common knowledge or that do not need to be kept secret given their significance." Identical language is used in the separate Patent Attorneys Code (Section 39a (2)). Virtually identical language is contained in the Federal Notaries' Code (Section 18). As noted above, the Legal Services Act, which came into force in 2008, includes a new category of legal professionals, "registered legal advisers." Although registered legal advisers are subject to contractual obligations to maintain confidentiality, the Legal Services Act does not include the same statutory professional secrecy requirements for registered legal advisers as those that apply to lawyers and other regulated professions. Registered persons are not monitored by public authorities as to their compliance with professional secrecy obligations, and any failure on their part to so comply is not subject to any sanctions under professional or criminal law. Given that registered persons are not subject to the same obligations of secrecy or privilege that apply to lawyers, their inclusion in the list of persons exempted from STR reporting for professional secrecy appears to be inappropriate under Interpretative Note 16.

945. The duties of confidentiality of auditors arise from Sections 323 HGB, 43, (1), sentences 1, 50, 56, (2), 57b and 62, (2) of the German Public Accountant Act (WPO), as well as Section 9 of the Professional Charter for Auditors and Chartered Accountants. They are criminally sanctioned by Section 203, (1) no. 3 of the German CC.

946. The duty of tax agents and tax advisers to maintain professional secrecy are contained in Section 57 paragraph 1 Tax Consulting Act which states: "Tax advisers and tax agents shall practice their profession independent, conscientious and with professional secrecy."

947. Under Section 203 of the CC, violations of professional secrecy carry criminal penalties of up to one year imprisonment or a fine.

948. The obligation to maintain professional secrecy is sufficiently serious that the CPC, the Civil Procedure Code, and the Tax Code each include provisions stating that persons subject to these obligations cannot be compelled to provide evidence about matters they came to know about under conditions of professional secrecy.

949. The general obligation of professional secrecy is binding unless overridden by another, specific exception provided for in law. The AML Act provides such an override in the case of reporting suspicious transactions. For lawyers and the other professions, the duty to report STRs (and, hence, override the obligation of professional secrecy) is qualified by the exceptions for providing legal advice and representing clients in court proceedings. The conflicting obligations – to report and to maintain professional secrecy – have or have not been satisfied. In practice, legal and accounting professionals tend to take a broad view of what is, and what is not, included in legal advice. In the case of notaries, almost all of their activities are considered to involve an element of legal advice since the work in attesting to the correctness of documents includes a determination that the terms of contracts and other documents are legally correct. Similarly, tax advisers are inclined to consider that much of their work, including preparing tax returns, involves legal advice on the clients' tax obligations.

---

<sup>71</sup> See paragraph 915 above for a discussion of the status of legal advisers.

950. Reporting practices of persons subject to professional secrecy obligations are also influenced by the threshold standard of “suspicion” set out in German law. As discussed under R. 13 above, the threshold for reporting suspicious transactions in Germany is somewhat higher than the standard of “reasonable grounds to suspect” that is called for in FATF Recommendation 13. As will be readily evident, the combination of a relatively demanding specification of suspicion, a carve-out for legal privilege and professional secrecy that extends across the legal and accounting professions, and a broad interpretation of what is considered to be legal advice have the cumulative effect of narrowing the range of transactions that are potentially reportable by the legal and accounting professions.

951. Section 11(4) of the AML Act stipulates that lawyers, patent attorneys, registered legal advisers, auditors and tax advisors “shall transmit the report (STR) to the competent federal professional chamber. Such chamber may comment on the report. It shall immediately transmit the report with its comments” to the competent law enforcement agency, with a copy to the BKA. This is the practice followed in each of the professions requiring membership in professional chambers. The arrangement is consistent with the provisions of paragraph 2 of Interpretative Note to Recommendation 16.

952. In practice, members of chambers make active use of the arrangements to file STRs through their federal chamber. The chambers report that members rely on the federal chamber to provide guidance on whether particular transactions do or do not satisfy the requirements for reporting. Members frequently seek advice as to whether the matter and the facts available satisfy the threshold set out in German law for reporting a transaction as suspicious. Members also seek advice on whether reporting would put the member in violation of his professional secrecy obligations. The chambers state that they only provide advice and do not “clear” the STR. Once an STR is submitted, it is forwarded promptly to the authorities, usually within 24 hours, and frequently with comments.

***Requirement to Make STRs on ML and TF to FIU (applying all the criteria of R 13 & IV to DNFBPs):***

953. Under Section 11 of the AML Act, all DNFBPs are required to file STRs. The specification of the standards for the obligation to make these reports related to suspicions of both ML and TF are the same as those for other reporters, as analyzed under Recommendation 13 above. Exceptions for legal privilege and professional secrecy impinge on the circumstances under which the legal and accounting professions are required to file STRs, as discussed in the introduction to this section.

***Protection for Making STRs and Prohibition Against Tipping-Off (applying c. 14.1-3 to DNFBPs):***

954. Protection for making STRs and Prohibition on tipping off are provided for in Sections 12 and 13 of the AML Act and are applicable to all covered persons, including DNFBPs. For analysis of these provisions, see the discussion and analysis of R. 14 above.

***Establish and Maintain Internal Controls to Prevent ML and TF (applying c. 15.1, 15.1.1 & 15.1.2 to DNFBPs):***

955. Section 9 of the AML Act sets out requirements for internal safeguards. In general terms, this section covers appointment of a compliance officer, internal controls, and employee training. These requirements do not apply fully to all DNFBPs and the gaps go beyond the discretion provided in Interpretative Note 15 to adjust the type and extent of measures “having regard for the risk of ML and TF and the size of the business.”

956. c.15.1 Compliance Management Arrangements. Article 2(1) of Section 9 of the AML Act (appointment of a compliance officer at management level) does not apply to DNFBPs, nor are there other requirements related to compliance management arrangements. The Explanatory Notes accompanying the AML Act state the exemption from the compliance officer requirement for nonfinancial institutions

“constitutes relief for small and medium-sized businesses in particular, which were previously required without exception to designate a compliance officer (money laundering).” The exemption from the requirement to appoint a compliance officer is inconsistent with Interpretative Note in 15 in several respects. The note requires that, for financial institutions, the compliance officer should be appointed at management level. The implication of the Notes is that, for other parties, the requirement is to have compliance management arrangements even if circumstances do not warrant appointment of a compliance officer. In addition, the exemption from the requirement to appoint a compliance officer is justified solely on the basis of giving relief to small- and medium-sized businesses. No consideration appears to have been given to the risk of ML and TF facing the parties exempted from the need to have a compliance officer. Further, the exemption extends to all nonfinancial institutions, not just small- and medium-sized businesses. Aside from the question of whether the small scale of many DNFBPs justifies appointment of a compliance officer, the Act does not specifically obligate DNFBPs to “develop appropriate compliance management arrangements,” as called for in c.15.1.1.

957. c. 15.1.2 Since DNFBPs are not required to have a compliance officer, the provisions of this criteria with respect to timely access to information are also not satisfied.

958. c.15.1 The safeguards enumerated in Articles 2(2) and 2(3) of the AML Act address the internal controls items required under c.15.1 and the training requirements under c. 15.3. The safeguards under 2(2) are: “developing and updating internal principles, appropriate business and customer-related safeguards and controls to prevent ML and TF. The safeguard under 2(3) is: “ensuring that employees responsible for carrying out transaction and for initiating and establishing business relationships are aware of methods of ML and TF and of the requirements pursuant to this Act. No provisions of the Act specifically address the c.15.2 criteria to have an audit function or the c.15.4 criteria to put in place screening procedures to ensure high standards when hiring employees.

959. While, in principle, these other internal safeguard provisions of Section 9, *i.e.* internal control and training requirements, apply to all DNFBPs, several professional chambers have exercised their discretion under the Act to exempt parties from these additional safeguards requirements if their firms employ 10 or fewer professionals.

960. Article 2(4) of the safeguards section of the AML Act allows supervisors to give instructions on the measures that are appropriate and necessary to implement safeguards. It also allows these instructions to be tailored to circumstances of individuals or groups of institutions or persons “on a risk-sensitive basis due to the type and amount of business conducted by such individuals or groups.” Under this authority, the Chamber of Lawyers, the Chamber of Notaries, the Chamber of Auditors, and the Chamber of Tax Advisers have all issued instructions exempting their members who are employed in firms of 10 or fewer professionals from the internal safeguard requirements of Section 9.

961. The AML Act provisions giving discretion to supervisors to give instructions on how safeguards are to be appropriately implemented on a risk-sensitive basis does not include any reference to ML or TF; it only refers to the “type and amount of business.” This is inconsistent with R 15 which states that the type and extent of measures “should be appropriate having regard to the risk of ML and TF and the size of the business.” Nor do the instructions by the Chambers to their members cite low ML and TF risk as a reason for the exemption. The explanation in the instructions issued by the Federal Chamber of Lawyers is: “in units of this size there is no risk of a loss of information relevant in terms of ML, something which may exist within larger company structures due to working methods involving the division of labor. The risk of the loss of information can be considered to be so small as to render the preventive measures to be taken to be disproportionate in terms of the effort and expense involved.” Similar explanations are included in the instructions issued by the other Chambers.

962. While the exemptions from safeguards requirements for members of Chambers has not been based on low risk of ML and TF, there was a general presumption that small firms of lawyers, auditors and tax advisers are probably less exposed to ML risk because they are more familiar with their clients. No risk assessment has been undertaken that might justify such a presumption.

963. Given the structure of the legal and accounting professions, the instructions exempting small firms from safeguard requirements are sweeping, covering the vast majority of professionals. While there are some large legal and accounting practices, small practices predominate. Notaries almost always work as sole practitioners and almost never in groups of more than two or three professionals. According to the Chamber of Tax Advisers, 75% of the 85 000 tax advisers are sole practitioners or work in firms of no more than 2 or 3 professionals. According to the Frankfurt Chamber of Lawyers there are approximately 150 000 lawyers in Germany, half of whom work in firms of 10 or fewer members. Audit firms tend to be somewhat larger, so it is likely that a minority of the 12 000 German auditors work in firms of 10 or fewer professionals.

### **Casinos**

964. Casinos are subject to the STR reporting obligations of Section 11 of the AML Act. They are also subject to the monitoring requirements under Section 3(4) of the Act. Although casinos are exempted from the requirement to have a control officer, they are subject to the other safeguard measures set out in Section 9 of the AML Act. All regulation and oversight of casinos is a *Länder* responsibility. There is no federal regulation of casinos. Based on discussions with the supervisors of casinos in Berlin and Hesse, it appears that regulatory requirements imposed on casinos by *Länder* generally do not include a specific anti-money laundering focus, although many of the rules with respect to integrity, financial control, and consumer protection overlap measures that would be needed for AML/CFT compliance. There are no specific requirements for casinos with respect to the internal control and audit function requirements under c.15.1 and c.15.2. Requirements to train staff are part of the casino regulatory framework and casino managers state that, under these requirements, they train staff in AML/CFT procedures and controls. Screening of owners, operators, and staff to prevent criminal involvement or unsuitability is also a standard element of casino regulation, and was well structured in the jurisdictions visited.

### **Real Estate Agents**

965. Real estate agents are subject to the STR reporting obligations of Section 11 of the AML Act. They are also subject to the monitoring requirements under Section 3(4) of the Act. Although real estate agents are exempted from the requirement to have a control officer, they are subject to the other safeguard measures set out in Section 9 of the AML Act. The real estate agency business is subject to business licensing requirements under the trade laws, which are administered at the *Länder* level. No official measures have been put in place to promote compliance by real estate agents with their obligations under the AML Act. Thus, none of the measures with respect to internal policies and controls, screening, training, and audit that are called for in R. 15 have been applied to real estate agents.

### **Dealers in Precious Metals and Dealers in Precious Stones**

966. The AML Act provisions with respect to STR reporting, monitoring, and internal controls—except for the requirement for a control officer—apply to dealers in precious metals and stones, and, more generally, to all dealers in goods, when they engage in transactions for cash of EUR 15 000 (USD 20 876) or more. Unlike the professions, small scale dealers in precious metals and stones have not been exempted from the AML Act requirement to establish internal safeguard (controls). These businesses are not regulated although they are subject to the trade laws that are administered by the states. No information was available on the AML/CFT practices of dealers in precious metals and stones. No measures have been



put in place to promote their compliance with their obligations under the AML Act, which includes the STR reporting obligation.

967. As is the case for FIs, there are no specific requirements for DNFBPs to pay special attention to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations. Nor is there a requirement to maintain written records of cases where such deficiencies are identified. For a discussion of the adequacy of these arrangements in Germany, see the analysis under R.21 above. The analysis there applies equally to DNFBPs.

### *Statistics (R.32)*

**Statistical Table 26: STRs Filed by DNFBPs**

	2004	2005	2006	2007	2008
Lawyers	11	11	3	5	9
Patent Attorneys	0	0	0	0	0
Notaries	1	1	0	1	5
Auditors	3	2	2	3	3
Tax Advisers	1	6	2	3	5
Real Estate Agents	0	0	1	0	0
Other Business Persons <sup>72</sup>	4	4	2	11	9
Casinos	5	6	4	7	4

### *Effectiveness of Implementation of STR Reporting and Internal Controls for DNFBPs*

968. Very few STRs are filed by any of the DNFBPs. To some extent, this seems to reflect an inadequate awareness of ML techniques and ML risks. Many of the DNFBPs visited had a narrow perception of ML and TF risks, focusing primarily on the placement stage to the neglect of more sophisticated techniques that may be used in the layering and integration stages of ML. A significant number of the DNFBPs visited took the view that if client funds were not handled, they would not be involved in ML transactions. Or that, if a sector were subject to regulation and clients were familiar, ML risk was low.

969. In the casino sector, there appeared to be inadequate awareness of the variety of ways casinos can be abused for ML purposes, as catalogued in the recent FATF report on vulnerabilities of the casino sector. Casino regulations do not sufficiently integrate AML/CFT controls into the regular control regime for casinos with the result that controls do not give sufficient priority to ML and TF considerations. In addition, although video recording systems are used, the general lack of live electronic surveillance systems limits the ability of casinos to monitor and detect ongoing activity that may be indicative of ML.

<sup>72</sup>

This category includes dealers in precious metals and precious stones.

970. No measures have been taken to promote AML/CFT compliance by the precious metals and precious stones dealers, or dealers in goods more generally. That, plus the lack of reporting and the general lack of information about the sectors' handling of cash transactions, suggests that there is little spontaneous compliance by precious metals and precious stones dealers with their obligations under the AML Act.

971. Real estate agents have a general awareness that they have responsibilities under the AML Act to report suspicious transactions, but appear to have only limited awareness of the various ways they could be used to facilitate ML. No official measures have been taken to promote compliance by real estate agents with their STR reporting obligations. That, coupled with the fact that virtually no STRs have been filed by real estate agents, suggests that there is little compliance with internal control, monitoring, and training requirements.

972. The effectiveness with which STR reporting criteria are being implemented in the legal and accounting professions requires a more nuanced evaluation. The very low volume of STRs filed by lawyers, notaries, auditors, and tax advisors suggests that they are not detecting and reporting suspicions of ML at a level that may reasonably be expected. The professionalism of the sectors as well as the various codes of conduct they must abide by means that these persons are generally more attuned to the need to follow policies and procedures to satisfy their regulatory obligations. Even with good internal controls, there are significant constraints on reporting. As described above, the combination of a relatively demanding legal specification of suspicion, a carve-out for legal privilege and professional secrecy that extends across the legal and accounting professions, and a broad interpretation of what is considered to be legal advice have the cumulative effect of narrowing the range of transactions that are potentially reportable by the legal and accounting professions. In addition, parties interviewed frequently displayed an underdeveloped appreciation for the multiple ways the legal and accounting professions can be misused for ML or TF. The professions have not yet organized themselves to undertake meaningful risk assessments of the sort recommended in the 2008 FATF risk-based assessment guidance papers. The general exemption of large sections of the legal, notary, auditing, and tax advisor professions from the sort of internal controls expected under R. 15 is an unhelpful relaxation of safeguards in sectors where there are already significant impediments to their playing a fully effective role in the AML/CFT regime.

#### **4.2.2. Recommendations and Comments**

973. In order to comply fully with Recommendation 16, Germany should do the following:

- DNFBPs should be required to have some form of risk-based compliance management arrangements.
- The authorities should undertake a systematic assessment of the ML and TF vulnerability of the DNFBP sectors.
- Authorities should develop programs to raise DNFBP's awareness of AML/CFT risks and improve DNFBP's ability to identify and report suspicious activities.
- Exemptions from the safeguards requirements of the AML Act, or blanket simplified procedures, should be based on evaluation of ML and TF risks.
- All DNFBPs should be subject to requirements to screen new hires for high standards, to train staff, and to have an AML/CFT audit function.
- All casinos, real estate agents, and dealers in precious metals and stones should be required to have AML/CFT internal controls.

- Authorities should review the scope of the carve-out from legal and professional privilege and the stringency of professional secrecy requirements with a view to permitting the professions to play a more forthcoming role in the reporting of suspicious transactions.

#### 4.2.3. Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16	NC	<ul style="list-style-type: none"> <li>• No requirement to have compliance management arrangements.</li> <li>• Discretionary exemption of most professions from safeguards based on firm size but not risk of ML or TF.</li> <li>• No risk assessments to justify safeguards exemptions or simplified measures.</li> <li>• In absence of safeguards, no training requirement.</li> <li>• No requirement to screen to insure high standards when hiring.</li> <li>• No audit function for DNFBPs.</li> <li>• No specific requirement for casinos to have AML/CFT internal controls or to have an audit function.</li> <li>• No supervisory framework for real estate agents and dealers in precious metals and stones and, hence, no specific requirements for internal policies and controls and screening and audit.</li> <li>• Inadequate awareness of potential ML vulnerabilities contributing to underreporting.</li> <li>• Inadequate risk assessment procedures among professions, leading to inadequate monitoring and underreporting.</li> <li>• Broad carve-out for legal and professional privilege combined with strict professional secrecy requirements place significant impediments to STR reporting.</li> </ul>

### 4.3. Regulation, Supervision, and Monitoring (R.24-25)

#### 4.3.1. Description and Analysis

##### *Legal Framework:*

##### **Casinos, Real Estate Agents, and Dealers in Precious Metals and Stones.**

974. Under Article 2 (11) of Section 2 of the AML Act, gambling casinos, real estate agents, and persons trading in goods are all subject to the preventive measures requirements of the Act and are required to be supervised. Each of these sectors is subject to *Länder*, but not federal, regulation. Under Section 16(9) of the AML Act, the competent authority for enforcing the compliance of casinos, real estate agents, and persons trading in goods with the Act is “the authority responsible under federal or state (*Land*) law.” Arrangements at the *Länder* level for designating the competent authority vary from *Land* to *Land*. A representative example is provided by Hesse. An ordinance has been issued assigning competency under the AML Act to the Office of the Regional Commissioner. Within the regional commissioner’s office, the task of insuring compliance is then delegated to a department with relevant skills and capacity. In the case of casinos, responsibility is assigned to the Department for Public Security and Order, a department whose

work is supervised by the Hesse interior ministry. Real estate agents and dealers in precious metals and precious stones (persons trading in goods) are assigned to another department in the Regional Commissioners' Office, one which has responsibility for administering the Trade Law and which is supervised by the Hesse economics ministry. Each *Land* has its own casino act and these laws designate an agency to act as casino supervisor responsible for licensing and oversight of casinos, with supervision of AML compliance being an additional responsibility as a result of Article 16(9) of the 2008 AML Act. In general, responsibility for casino supervision and AML compliance lies with *Land* interior ministries or subordinate authorities. In two, *Länder* responsibility lies with the finance ministry. As of the time of the assessment, responsibility for AML/CFT compliance under the 2008 AML Act had not been definitively decided in three *Länder*. While responsibility of the designated casino supervisor for AML compliance is relatively clear, this function does not appear to be well developed. There is no similar clarity with respect to the AML duties of the other departments of the Offices of the Regional Commissioner which have been assigned responsibility for real estate agents and persons trading in goods. These offices are thinly staffed, have responsibility for administering numerous laws, and typically have no particular knowledge of ML matter or of the details of the sectors assigned to them.

### **Lawyers, Patent Attorneys, Notaries, Registered Legal Advisers, Auditors, and Tax Advisers**

975. Under the AML Act, lawyers, patent lawyers, notaries, registered legal advisers, auditors, and tax advisers are all subject to the preventive measures provisions of the Act and are required to be supervised. Section 16(2) of the Act designates competent authorities in each of these professions for purposes of enforcing the Act.

- For lawyers and legal advisers who are members of Chamber of Lawyers, the competent bar association.
- For patent attorneys, the Chamber of Patent Attorneys.
- For notaries, the president of the regional court of the district where the notary is based.
- For auditors and chartered accountants, the Chamber of Auditors
- For tax advisers and tax agents, the competent Chamber of Tax Advisers.

976. Each of these professions is a regulated profession governed by a federal statute and requiring membership in a professional chamber. Except for the notaries, the appropriate chamber acts as the SRO supervisor for the AML/CFT compliance of its membership.

### ***Regulation and Supervision of Casinos (c. 24.1, 24.1.1, 24.1.2 & 24.1.3):***

977. Each *Land* has its own casino act. As discussed under R 12, a Gambling Treaty was adopted by the 16 *Länder* and came into force in 2008. One of the principal objectives of the Treaty (Objective 4) is "To ensure that gambling is conducted in an orderly fashion, that the gamblers are protected from fraudulent activities, and defenses are in place against the criminality that accompanies and follows gambling. Most of the acts on casinos were amended around the time the Gambling Treaty was introduced and, as a result, most of the 16 different casino acts are now similar, including with respect to AML provisions. These casino acts incorporate AML provisions based on the earlier AML Act. Even without updating to reflect the 2008 AML Act, *Länder* supervisors have responsibility for ensuring compliance with all relevant laws so compliance with the new Act is within their responsibility.

978. As an illustration, under the Hesse Casino Act:

- Art 15 provides for supervision of casinos under the responsibility of the Interior Ministry and lists the objective of casino supervision is to ensure that operations are correct in economic terms;
- Art 15.2 provides for the specific supervision, as now required under Section 16 of the AML Act (c.24.1);
- Art 15 lays out conditions for casino operations, including that casino owners and operators must be licensed, that casinos can only operate in fixed locations, that identification of clients is required when they buy Euro or more in chips and that clients may be identified independently as they buy chips, *i.e.* upon entry (c.24.1.2);
- Art 4 and Art 5 require that both the owner and the operator must be authorized. The operator must: have sufficient resources, sufficient knowledge, be able to assure proper operation, prove the legal source of his wealth upon request, be subject to a police background clearance, and any changes in shareholders must be notified (c.24.1.3);
- The casino supervisor has authority to issue orders or take any other measures necessary to fulfill his duties, up to and including revoking a license. Under the AML Act, Section 16 the competent authority (the Ministry of Interior) can impose fines of up to EUR 50 000 (USD 69 585) for specified administrative offenses under the Act and up to EUR 100 000 (USD 139 170) in the case of other specified administrative offenses (c.24.1.1); and
- Other sections require internal safeguards including: (a) compliance officer, (b) internal principles (*i.e.* internal control framework), (c) training, (d) monitoring, and (e) vetting.

### ***Analysis of Effectiveness***

979. Based on discussions with casino supervisors and casino operators in Hesse and Berlin, it appears that only some of the AML elements of the supervisor framework are being adequately administered. Licensing requirements are energetically enforced, including the requirement for police background checks for owners, operators, and senior managers, as well as the requirement for casino employees to get a certificate from the police stating that they do not have any criminal violations. The primary focus of supervisor concern is financial controls, although AML aspects are not overlooked. Safeguard provisions are required but effective implementation appears to be spotty; on-site monitoring falls primarily to fiscal authorities with a focus on financial control and collection of tax revenue. The procedures for identification of customers, which are set out in the AML Act, appear to be carefully followed, but procedures for monitoring and detecting, with limited attention to observing activity that may indicate attempts at ML, do not appear to be well-developed. While staff and managers are given training in monitoring for indications of ML, casino representatives did not appear to have an awareness of the variety of ways casinos could be exploited by money launderers, as catalogued in the recent FATF Report on vulnerabilities of the casino sector. With identification only required upon entry, no formalized systems are required, or in place, to be able to link CDD information for a particular customer to the transactions that the customer conducts in the casino. Visual monitoring by staff is relied on for monitoring which clients engage in which transactions. Supervisory attention for AML purposes appears to focus on verifying that identification procedures are being followed.

**c.24.1 Monitoring Systems for Other DNFBPs (c. 24.2 & 24.2.1):****Real Estate Agents and Dealers in Precious Metals and Precious Stones**

980. As noted above, supervisory responsibility for AML/CFT compliance by real estate agents and dealers in precious metals and precious stones is a *Länder* responsibility. As illustrated by the situation in Hesse, most *Länder* appear to have taken formal steps to formally assign the AML/CFT supervisory responsibility for these sectors to an administrative body of the *Länder* government, typically a department of the Regional Commissioners Office. These departments typically have responsibility for administering a wide variety of laws and regulations with relatively few staff, and no training or familiarity with ML issues. Based on discussions with *Länder* officials and with the two sectors, it is evident that no effective steps have been taken to promote, let alone supervise and enforce, compliance with AML/CFT requirements in the two sectors.

**Lawyers**

981. Under the Federal Statute on Lawyers, the regional chambers of lawyers are the bodies responsible for regulating the professional obligations of lawyers. (The Federal Chamber of Lawyers is an umbrella organization for the 28 regional chambers of lawyers; it does not have a regulatory function.) AML/CFT compliance is one of the professional obligations of lawyers and the regional chambers are the SRO supervisors of their members. The legal provisions governing the chambers' supervisory functions are contained in the Federal Statute on Lawyers. Members are required to submit to the discipline of the chamber.

982. Based on discussions with regional chambers of lawyers in Hesse and Berlin, the essential first pillar of the ensuring lawyers' compliance with their AML/CFT obligations is to ensure that they have knowledge. With this objective, the regional chambers, supported by the Federal Chambers, have sent notices to members explaining provisions of the AML Act and published a paper on indicators of ML. Information from the BKA is published on the chambers' websites, as well as links to the secure web information are available on BKA's website and other data sources on ML. A guidance manual is under preparation.

983. The chambers do not have authority to conduct routine compliance examinations of members' offices. However, the chamber can conduct investigations, including examination of members' files, if appropriate, in response to complaints or on the basis of other indications of infractions. Such inspections could include investigation of compliance with AML/CFT obligations. No statistics were available on the number of such inspections that have been conducted. The inability of the chambers of lawyers to conduct routine or spot checks of compliance is inconsistent with c.24.2.1.a of the methodology, which calls for SROs to have adequate powers to perform its functions, including monitoring compliance.

984. The Federal Statute on Lawyers sets out the disciplinary sanctions available to the chamber if professional rules are breached. In minor matters the chamber has the right to reprimand members. In more serious matters the Statute provides for a Lawyers' Disciplinary Court, or for a Higher Lawyer' Court, or even referral to the Federal Supreme Court. The sanctions available to the Lawyers' Disciplinary Court include: (i) a warning, (ii) a caution, (iii) a fine of up to EUR 25 000 (USD 34 793), (iv) a ban for a period of one to five years, and (v) exclusion from the profession. Higher Lawyer' Courts hear appeals of judgments of the disciplinary court.



## Patent Attorneys

985. Under the Federal Statute of Patent Attorneys, the Chamber of Patent Attorneys is responsible for monitoring compliance of patent attorneys with their professional obligations. AML/CFT compliance is one of those obligations. There is only one, national chamber of Patent Attorneys. The legal provisions governing the supervisory responsibility of Chamber of Patent Attorneys are set out in the Statute. The supervisory arrangements, practices, and powers of the Chamber of Patent Attorneys parallel those of the Chamber of Lawyers in almost all respect, including the range of sanctions.

## Notaries

986. Under the Federal Statute on Notaries, notaries are holders of a public office and as such exercise public duties. Thus, the President of the Regional Court, not the Chamber of Notaries, is the supervisory authority for notaries who have business offices within the district of the Regional Court. This person is a judge who is particularly familiar with the specific legal regulations for notaries. He or she may assign other judges to assist with the fulfilment of his or her tasks. Notaries are required to undergo a full examination of their practices at least once every four years. Judges conduct on-site examinations of the offices of notaries and have access to all the files of the notaries. On-site examinations typically last two or more days and include review of AML/CFT compliance. A report of examination is produced, including a section on AML/CFT compliance.

987. If the report finds deficiencies, the notary will be requested to comment on them and to resolve the deficiencies. The supervisory body may conduct further inspections to verify whether the deficiencies have been rectified.

988. In the case of serious deficiencies, specific sanctions are available under the AML Act for defined administrative offenses and a range of supervisory measures and sanctions are available under the Statute on Notaries:

- For less serious matters, an admonition or statement of disapproval,
- Reprimand,
- Fine of up to EUR 50 000 (USD 69 585), or in certain cases of inappropriate benefit, a fine of up to two times the benefit even if that exceeds EUR 50 000,
- Removal from current official office, and
- Permanent removal from office.

## Auditors

989. Under the Professional Accountants Statute, the chamber of auditors is the body responsible for regulating the professional obligations of auditors. There is only a single national chamber of auditors. AML/CFT compliance is one of the professional obligations of auditors, and for clarity, the Law on Audits now cross references the relevant provisions of the AML Act. Under the AML Act, the chamber is the designated competent SRO authority for supervision of AML/CFT compliance of auditors. The legal provisions governing the chambers' supervisory functions are contained in the Professional Accountants Statute. Members are required to submit to the discipline of the chamber.

990. The Chamber of Auditors exercises two forms of supervision: disciplinary professional supervision and preventive supervision. Under disciplinary professional supervision, on the basis of complaints or other indications of infractions, the chamber may investigate the activities of the auditor including requiring documents to be presented or through on-site examination of files. These procedures may include examination of compliance with AML/CFT requirements. Where deficiencies are identified, a range of sanctions is available under the Professional Accountants Act including:

- Reprimand,
- Fines of up to EUR 50 000 (USD 69 585), and
- In serious matters, review by a special court with authority to impose fines of up to EUR 500 000 (USD 695 850) or to impose a temporary or permanent ban.

991. In addition to the sanctions available under the Professional Accountants Act, for administrative offenses specified in the AML Act, the relevant competent authority may impose the EUR 50 000 and EUR 100 000 (USD 69 585 and USD 139 170) fines allowed for in Section 16 of the Act.

992. Under its preventive supervision, the chamber has developed a quality assurance program which focuses on the quality of the audit function. Several reviews are conducted under this program. Once every six years, auditors are required to undergo an intensive on-site review of their audit work to assure that it is being done in an adequate manner. In addition, under the quality assurance program, all auditors are subject to a spot, unannounced inspection at least once every three years. Audit procedures include steps to cover AML/CFT compliance so the quality assurance program, although its focus is on the quality of audit work, also provides an opportunity to verify AML compliance. If deficiencies are identified in the course of a quality assurance examination, these may be referred to the disciplinary process for action.

### **Tax Advisers**

993. Under the Tax Consulting Act, the Chamber of Tax Advisers is the body responsible for regulating the professional obligations of auditors. There are 21 regional chambers and a Federal Chamber of Tax Advisers, to which all regional chambers belong. Under the Tax Consultant Act, a single code of conduct governs all tax advisers. By-laws providing instructions on the application of legal obligations are issued under the authority of regional chambers, but are required to be uniform across the country. AML/CFT compliance is one of the professional obligations of auditors. Under the AML Act, the chamber is the designated competent SRO authority for supervision of AML/CFT compliance of auditors. The legal provisions governing the chambers' supervisory functions are contained in the Professional Accountants Statute. Members are required to submit to the discipline of the chamber.

994. The regional chambers, in cooperation with the federal chamber, have taken a number of steps to promote compliance with the requirements of the AML Act. On enactment, information was circulated to members on the requirements of the new law as it impacted tax advisers. In April 2009, the chambers published a guide to the AML Act, including recommendation as to how tax advisers could implement required measures. Additionally, the websites of both the regional and federal chambers provide information and notices on AML/CFT issues, including typologies, information on new methods, and reports from BKA. In addition to website publication of AML/CFT materials, both the regional chambers and the federal chamber have journals and weekly newsletters that include current topics related to ML.

995. The regional chambers do not have authority to conduct routine examinations of tax advisers. On the basis of complaints or other indications of infractions, the chamber may conduct investigations to resolve or correct deficiencies. These examinations may include request for documentation or on-site

examinations of tax adviser records. Such examinations may include review of AML/CFT compliance. The inability of the chambers of tax advisers to conduct routine or spot checks of compliance is inconsistent with c.24.2.1.a of the methodology, which calls for SROs to have adequate powers to perform its functions, including to monitor compliance. Where, on the basis of investigation, AML deficiencies are identified, the Tax Consultancy Code has provisions for the same range of sanctions as are available to the Chamber of Auditors under its authorizing legislation. For administrative offenses under the AML Act, the regional tax office is the competent authority for imposing the sanctions provided for in Section 16(1) and (2).

***Guidelines for DNFbps (applying c. 25.1):***

996. Guidelines were issued in 2006 by the BKA for the liberal professions (self-employed professionals) covered by the previous Act. The general provisions describing what ML is still have general applicability. Guidelines covering implementation and compliance with the 2008 AML Act are being developed and issued by the various professional chambers. In April 2009, Guidelines were issued by the Federal Chamber of Tax Advisers and the regional chambers. In May 2009, the Chamber of Notaries issued similar Guidelines, as did the Chamber of Patent Attorneys. Guidelines are under development by the Federal Chamber of Lawyers and the Chamber of Auditors. (Since the new guidelines were only issued at the time of the assessment, and only in German, a qualitative evaluation of the content of these new guidelines is beyond the scope of this assessment.) No comparable guidelines are available for casino operators, although some regional casino supervisors have issued instructions on the specific AML requirements applicable to casinos, including information on activities that may be suspicious. No guidelines have been prepared for real estate dealers or dealers in precious metals and stones.

***Feedback (applying c. 25.2):***

997. The FIU provides a range of feedback to all reporting parties, including topics of specific relevance to DNFbps. In October 2003, the FIU published a paper, ‘Possible ML indications in accordance with Section 261 of the CC relevant to newly obliged parties,’ which provided numerous indicators of potential ML practices in the DNFbps. Updated information is provided in periodic Situation Reports issued by the FIU. In addition, the annual FIU report includes discussion of recent trends and statistical analysis of STR reporting by different sectors.

998. Lawyers, patent attorneys, registered legal advisers, auditors, and tax advisers all file their STRs with their respective federal professional chambers. The various chambers report that members rely on the federal chambers to provide guidance on whether particular transactions do or do not satisfy the requirements for reporting. Members frequently seek advice as to whether the matter and the facts available satisfy the threshold set out in German law for reporting a transaction as suspicious.

***Adequacy of Resources – Supervisory Authorities for DNFbps (R.30)***

999. Professional chambers all have adequate resources to carry out their AML/CFT compliance monitoring responsibilities. Chambers are funded by contributions of members and the contributions are set at a level that makes it possible for the regional chambers to perform their supervisory functions. In addition to professional staff employed by chambers, as SROs, much of the supervisory function is carried out by chamber members or committees of chamber members.

1000. Casino supervisors are officials of *Länder*. Their offices appear to be adequately staffed and resourced, in part because their functions include significant revenue collection.

1001. The departments of Regional Commissioners Offices assigned responsibility for oversight of AML compliance by real estate agents and those responsible for dealers in precious metals and stones (more generally, persons trading in goods) have received no additional resources to carry out these additional duties, nor do they have training or experience in ML matters. They are frequently stretched to carry out their day-to-day responsibilities other than on an ad-hoc basis.

***Effectiveness of implementation of supervision for DNFBPs.***

1002. Implementation of supervision varies significantly across the different DNFBP sectors. In the case of real estate agents and dealers in precious stones, there is effectively no supervision, although a formal legal framework exists. The same is true for independent TCSPs. Although the focus of casino supervisors is primarily on financial controls, an AML supervisory framework for the sector is reasonably well established with an emphasis on licensing, integrity of owners, operators and staff, and on customer identification upon entry. Less attention appears to be directed to ensuring that casinos have effective policies and controls to monitor, detect, and report activities that may be ML-suspicious. In comparison, the regulatory organizations for the professions have much more highly-structured arrangements for monitoring and enforcing compliance with AML/CFT obligations and professional obligations more generally. But even among the various professions, there is considerable unevenness in the quality and thoroughness of oversight. All chambers emphasize awareness raising and each has issued a variety of notes, guidance and background information on AML/CFT compliance, and very recently begun to issue formal guidance. Direct compliance monitoring of notaries, which is carried out by judges, is the most thorough since it includes periodic on-site examination that includes a specific section on AML compliance and allows for review of files and a written report of examination. The chamber of auditors' quality assurance program, although focused specifically on audit quality, provides an opportunity for a periodic examination of AML compliance. The practices of the regional chambers of lawyers, the chamber of patent lawyers, and the regional chambers of tax advisers do not allow for periodic on-site examination of files so there is no systematic, independent check on whether these professions are or are not complying with their preventive measures obligations. Inspections conducted in response to complaints or other indications of infractions allow detection of weak AML practices in particular cases, but do not provide a basis for evaluating the general effectiveness of implementation of preventive measures, as contemplated in c.24.2.

1003. For covered parties, the AML Act introduces risk-based considerations in a systematic way. Risk sensitivity depends on the type of contracting party, business relationship, product, or transaction. (AML Act, Section 2.4). Section 2.4 also provides: "The institutions and persons covered by this Act shall be able to demonstrate to the competent authorities mentioned in Section 16(2) that the extent of the measures is appropriate in view of the risks of ML and TF." In general, risk assessments are not well developed among the professions, although some information has been circulated on how such assessments can be handled. With the exception of notaries and auditors, where explicit authorization is made for periodic routine on-site inspections, the other professions (lawyers, patent attorneys, tax advisers) are restrained by professional secrecy rules in their ability to "demonstrate to the competent authorities" that their risk-based measures are appropriate.

1004. c.24.2 DNFBP supervisors have not yet developed systematic risk assessment procedures to guide them in evaluating whether the systems for monitoring and ensuring compliance are appropriate given the risk of ML or TF in the sector. In the absence of a systematic evaluation of risk, decisions to relax measures required of professions appear to have been taken on the basis of supervisory burden or administrative convenience. As noted above, the AML Act exempts DNFBPs from the requirement to appoint a compliance officer at management level, with the explanation that this "constitutes relief for small and medium-sized businesses in particular." Similarly, supervisors have exempted lawyers, notaries, auditors, and tax advisors who are employed in firms of 10 or fewer from the general obligation to adopt

internal AML/CFT safeguards. The exemption is based on the type and amount of business done by these groups, without consideration of whether such business is vulnerable to ML or TF. The explanation for the exemption provided by the Federal Chamber of Lawyers states that “in units of this size there is no risk of a loss of information relevant in terms of ML, something which may exist within larger structures due to working methods involving the division of labor. The risk of the loss of information can be considered so small as to render the preventive measures to be taken to be disproportionate in terms of effort and expense involved.”

#### 4.3.2. Recommendations and Comments

1005. In order to comply fully with Recommendations 24 and 25 (cr. 25.1), Germany should:

- Clarify *Länder*-level AML/CFT supervisory responsibility for real estate agents and persons trading in goods and ensure adequate resources and capacity to carry out these responsibilities.
- Strengthen AML/CFT supervisory capacity of casino supervisors.
- Take steps to ensure that Chambers of Lawyers, the Chamber of Patent Lawyers, and Chambers of Tax Advisors have adequate authority to conduct routine AML/CFT compliance monitor of their members.
- Authorities should issue up-to-date guidance for all DNFBPs
- Authorities should carry out AML/CFT risk assessments of the various DNFBP sectors, maintain them up to date, and make sectors aware of risks.

#### 4.3.3. Compliance with Recommendations 24 & 25 (criteria 25.1, DNFBP)

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
R.24	NC	<ul style="list-style-type: none"> <li>• Inadequate supervisory authority and capacity with respect to oversight of real estate agents and persons trading in precious metals and stones.</li> <li>• Insufficient supervisory oversight of AML compliance by casino operators.</li> <li>• No authority for Chambers of Lawyers, Chamber of Patent Attorneys, and Chambers of Tax Advisors to conduct routine compliance monitoring of members.</li> <li>• Compliance monitoring and enforcement generally ineffective, including:               <ul style="list-style-type: none"> <li>○ Lack of awareness of ML risks in casinos.</li> <li>○ Risk assessments have not been developed by the competent authorities responsible for monitoring and ensuring compliance with AML/CFT requirements.</li> </ul> </li> <li>• Insufficient resources and capacity for supervisors of real estate agents and dealers in precious metals and precious stones.</li> </ul>
R.25	PC	<ul style="list-style-type: none"> <li>• Guidelines for lawyers, auditors have not been updated; no guidelines for dealers in precious metals and stones and real estate agents.</li> </ul> <p>Rating for this section: <b>PC</b></p>

#### 4.4. Other Non-Financial Businesses and Professions – Modern-Secure Transaction Techniques (R.20)

##### 4.4.1 Description and Analysis

###### *Legal Framework:*

###### *Other Vulnerable NFBPs (applying R. 5, 6, 8-11, 13-15, 17 & 21 c. 20.1):*

1006. Germany has chosen to apply the preventive measures requirements of the Recommendations to the following non-DNFBP nonfinancial businesses and professions: all persons trading in goods, financial advisers, and “financial enterprises” that are investment advisers. Financial enterprises are under the supervision of the BaFin. Inclusion of these nondesignated, nonfinancial businesses and professions conforms to requirements under EU directives.

###### *Modernization of Conduct of Financial Transactions (c. 20.2):*

1007. c. 20. 2 In Germany, the share of cash payments in retail trade is steadily declining. This trend is the result of innovations in the financial system and specific measures adopted by the German authorities. In 1994, cash transactions in retail trade accounted for 78.7% of turnover, but by 2008, it had fallen to 60.4%. Based on recent trends, industry analysts anticipate that by 2015, noncash payments will account for 50% of retail trade. Electronic payments in Germany are above the EU average; Germany accounts for approximately 23.5% of all electronic payments in the EU, a share which is somewhat larger than Germany’s share of EU GDP.

1008. The various types of noncash payment instruments in use include: credit transfer, direct debit, card payments, e-money, payment by check, and others. More than 80% of all noncash payments are made by credit transfer and direct debit, which are always done via bank accounts. Checks are little used.

###### *Trends in card usage:*

1009. The transactions conducted in Germany using credit cards are rising steadily. In 1998, credit card transactions in Germany totaled EUR 28.6 billion (USD 39.8 billion); by 2007, it reached EUR 54.3 billion (USD 75.6 billion). At the same time, the number of credit cards issued by suppliers also grew considerably between 1998 and 2007.

1010. Card payments consist essentially of payments by credit card, Electronic Cash (ec-cash or *PIN-verified payments*), EC direct debit (*signature-verified card payments*) and Maestro. “Electronic cash,” “EC direct debit” and “Maestro” are debit cards. Of a total retail trade turnover of EUR 360 billion (USD 501 billion) in Germany in 2008 (not including motor vehicles, mineral oil, pharmacies, mail-order trade), the card turnover amounted to EUR 130 billion (USD 181 billion), or a share of 36.1%. The turnover per type of card was 30.1% for debit cards—of which 17.9% for electronic cash, 12% for EC direct debit, 0.2% for Maestro—and 5.2% for credit cards. Shop-issued cards with a payment function accounted for a share of 0.8%. Purchases on account or by installment and other types of payment accounted for only 3.5%.

1011. In recent years, the EC cash procedure (*PIN-verified payments*) has continued to grow and use of the EC debit procedure (*signature-verified card payments*) has decreased. Here, it should be noted that both of these procedures, *i.e. signature-verified card payments* and *PIN-verified payments*, are noncash means of payment and, thus, with both procedures, the payment is booked via a bank account. The only difference between the two is that with *PIN-verified payments*, the issuer of the card guarantees the



payment and with *signature-verified card payments*, the payment risk lies solely with the creditor of the payment. As regards ML, the difference between the two is thus irrelevant; both procedures are equally secure.

1012. Surveys show that 25% of large enterprises intend to make modifications in their payment transactions infrastructure before the end of the year 2009. An additional 35% have announced that they intend to do so in the following years. Technical requirements for card payments have changed as a result of the introduction of the Single Euro Payment Area (SEPA). In addition, traders' IT managers face new challenges in dealing with procedural innovations such as "no-contact payment", "fingerprint identification", "mobile phone payment", "self-payment", or "digital signature registration".

1013. The total defaults registered within the framework of the signature-based EC direct debit procedure (payment amount could not be collected) came to 0.057% all told in the year 2008, down substantially from a peak figure of 0.123% in the year 2004 and a significant improvement for the fourth year in a row. Utilization of the blocked-card or trader notification database of the network operator has been a major factor in the decline in debit default. Furthermore, use of the KUNO platform (see below) has helped significantly to curb criminal defaults in the EC direct debit procedure.

#### ***Trends in use of online banking and payments:***

1014. Of some 93 million current accounts in Germany, almost 40 million are now used via online banking:

**Statistical Table 27: Number of online accounts according to the statistics of the *Deutsche Bundesbank* (in EUR millions)**

	2000		2001		2002		2003		2004	2005	2006		2007	2008					
<b>Credit banks</b>	8.5	56%	10.1	53%	13.7	46%	14.0	45%						15.9	45%			15.2	38.6%
<b>Regional banks and savings banks</b>	4.2	28%	5.5	29%	11.1	37%	11.1	36%						11.7	33%			13.8	35.1%
<b>Credit co-operatives</b>	2.4	16%	3.6	19%	4.8	16%	5.6	18%						7.7	22%			10.3	26.2%
<b>Total</b>	<b>15.1</b>		<b>19.1</b>		<b>29.7</b>		<b>30.8</b>		<b>33.1</b>	<b>33.3</b>	<b>35.3</b>		<b>33.2</b>	<b>39.3</b>					

#### ***Measures to improve payments processing in Germany***

1015. Single Euro Payments Area (SEPA): With a view to making payments systems in the European Union more modern and more secure, Germany actively supports the *Single European Payments Area* (SEPA) project, which aims to standardize payments in the EU. The legal framework for SEPA was created under Germany's presidency of the Council in 2007, in the form of *Directive 2007/64/EC of the European Parliament and of the Council of November 13, 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC* (known as the Payment Services Directive). Germany implemented the Directive in its national law by means of the Payment Services Implementation Act (*Zahlungsdienstleistungsgesetz*) of June 25, 2009 and the Act Implementing the Consumer Credit Directive, the Civil-Law Component of the Payment Services Directive as well as Restructuring the Provisions on the Right of Withdrawal and Return (*Gesetz zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdienstleistungsrichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht*) of July 29, 2009. Both of

these German laws entered into force on October 31, 2009. Alongside this legal framework, SEPA provides for innovative cashless payment products, which have been newly developed by the banking industry (the products are the SEPA Credit Transfer, SEPA Direct Debit, and SEPA Card Payment). The SEPA Credit Transfer has already been available since January 2008; the SEPA Direct Debit was launched on November 1, 2009. When it comes to SEPA Card Payments, so-called “rulebooks” are available, which give specifications for this product. However, the product itself has not yet been introduced to the market. Customers’ needs were taken into account when developing these new payments products, making them customer friendly and well-attuned to their specific users. Moreover, the SEPA products are offered at attractive prices. It is thus fair to assume that these means of payment will be widely used by customers and, as a result, many payments that are made in cash will henceforth move over to a noncash basis by means of the SEPA products.

1016. In addition to this, direct debit (*Lastschriftverfahren*) plays a pronounced role in Germany, accounting for 48.3 percent of all cashless payments in 2007. Germany has by far the largest market for direct-debit payments in the European Union (with 7.982 billion payments in 2008). In future, new business in this area will be based on the SEPA standards.

**Amendment of section 69(1) of the Act on Compulsory Sale by Public Auction and Compulsory Receivership (*Zwangsversteigerungsgesetz – ZVG*):**

1017. A further example of the Federal Government taking measures to prevent the use of large amounts of cash in areas at threat from ML, while simultaneously using effective government control mechanisms, is the amendment of Section 61(1) of the above-named Act (here: Compulsory Sale Act). As a result of the amendment to Section 69(1) of the Compulsory Sale Act, collateral for the compulsory sale of immovable property may no longer be provided in cash.

1018. In the compulsory sale procedure for immovable property, it is a general rule that the creditor conducting the procedure requires collateral from every bidder. This collateral is equal to 10% of the market value of the property and must be provided immediately after the submission of a bid. The bid only becomes effective once the collateral has been provided. If the collateral is not paid, the bid is rejected and ceases to exist. Unsuccessful bidders receive their collateral back once the procedure is completed. The winning bidder’s collateral is kept and offset against the sale price.

1019. Before the amendment to the Act, the collateral was usually provided in cash. This made it possible, for example, to launder untaxed cash or cash of illegal origin through the sale process, either by buying the property (laundering on the part of the successful bidder) or by providing and then receiving back the collateral (laundering on the part of the unsuccessful bidder). As a rule, the collateral was repaid by means of a transfer to the account of the person who had provided it. In this way, money of illegal origin was injected into the financial system and the person who provided the collateral was furnished with a spurious explanation as to a legal source for the money.

**Number of compulsory sale procedure per year**

2004	2005	2006	2007	2008
87 190	91 846	87 833	87 365	82 870

1020. To promote cashless payments at courts’ payment offices and to help prevent ML, cash payments have generally been excluded from the compulsory sale procedure since the Compulsory Sale Act was amended on December 22, 2006 (Section 69(1) of the Compulsory Sale Act). The required collateral can only be provided in the form of a check verified by the *Bundesbank*, a crossed check issued by a credit

institution authorized to do so, or a declaration of surety from such a credit institution (Section 69(2) and (3) of the Compulsory Sale Act).

***KUNO (crime control in noncash payment transactions through the involvement of non-police organizations: Kriminalbekämpfung im unbaren Zahlungsverkehr unter Nutzung nichtpolizeilicher Organisationen)***

1021. *KUNO* is a joint platform involving the police and the retail trade that is intended to reduce the misuse of lost or stolen debit cards. The centerpiece of this platform is a **central blocked-card database** containing information about the reported loss or theft of cards. In 2001, the system was initially rolled out on a regional basis and was extended to cover the whole of Germany in 2006.

1022. The blocked card database contains information about the reported loss or theft of cards that is provided by police offices in all of the federal states in Germany in order to prevent promptly the use of these cards at companies participating in the system, especially the retail trade. To this end, bank data (the sort code, account number and, if known, card issue number) are reported to the *KUNO* database. Access to the police's nationwide and centralized *KUNO* application is provided via a police crime prevention program's server in a police extranet ([kuno.extrapol.de](http://kuno.extrapol.de)). The police's extranet allows every police officer to access the *KUNO* application and block cards. Users can enter data and report stolen credit cards using a standard browser interface (such as Internet Explorer or Netscape). The card data are encrypted automatically and sent via email to the central notification unit for the retail trade, which sends the blocked card reports to the individual network operators and retail stores.

1023. Since *KUNO* was introduced on a nationwide basis in 2006, the number of cases and amount of the losses arising from fraud involving stolen or otherwise misappropriated debit cards has been reduced significantly. In 2008, a marked decrease was achieved in this way, with the number of cases registered down by 24.6% to 21 820.

***Measures to reduce the use of cash in the tax administrations of the Länder***

1024. Organizational measures have been implemented in the tax administrations of the *Länder* in order to reduce the use of cash. The tax administrations of the *Länder* are responsible for levying and collecting a large share of Germany's taxes. Over the last 10 years, the option of using cash to pay taxes due has gradually been reduced. Today, taxes are paid on a purely cashless basis, that is, their processing always involves a bank account.

1025. Of all payment transactions, around 50 percent are carried out by account transfer, around 45% by direct debit (this form is growing in popularity) and around 5% by check (this form is in decline). The only exception is in the area of enforcement, where cash payments are still accepted in some cases for outstanding tax debts. However, the sums of money concerned are generally small. Nonetheless, this last area is also undergoing restructuring, as there are plans to allow the use of credit cards to pay off outstanding tax debts as part of the enforcement procedure in the future.

***Use of large denomination bank notes***

1026. As Germany is a member of the European Monetary Union (EMU), the largest banknote circulating in Germany is the EUR 500 (USD 696) note, issued by the ECB. While aggregate statistics on the stock of such notes are published by the ECB, reliable statistics are not available on the share of such banknotes that circulate within Germany. The ECB publishes statistics showing the volume of Euro banknotes attributable to each EMU member, but these statistics are based on a fixed formula which distributes a proportionate share of the outstanding banknotes to each member based on the size of the balance sheet of each national central bank. The resulting allocations do not have any necessary relation to

the volume of such banknotes actually in circulation in any country within the EMU, as such notes readily migrate across member countries and circulate widely outside the EMU. However, it should be noted that specialized counting machines used by some Euro system central banks do allow more accurate estimates of the volume of large denomination bills circulating within their national boundaries.

1027. The German authorities note that, under the EC Treaty establishing the ECB, the ECB has the exclusive right to authorize the issuance of banknotes within the Euro area, and both the ECB and the national central banks are allowed to issue banknotes. Further, neither the ECB nor national central banks may take instructions from EU institutions, bodies, offices or agencies, from any government of a member state or from any other body. Thus, it is for the ECB Governing Council to decide independently what banknote denominations may be issued. As a general rule, Germany is extremely hesitant to take any action that could give rise to even the impression of disregarding such independence and has consequently refrained from requesting that the ECB reconsider its policy with respect to authorization of large denomination bank notes.

1028. With due regard for the independence of the ECB, there appears to be some scope for Germany to take some specific measures to limit the use of high-denomination bank notes within Germany. It is worth noting that not all central banks within the Euro system print or issue EUR 500 bank notes (or even EUR 200 notes). In addition, it can be noted that in some countries, the retail sector has decided that large denomination bank notes will no longer be accepted (just as small denomination coins are no longer accepted.)

#### **4.4.2. Compliance with Recommendation 20**

	<b>Rating</b>	<b>Summary of factors underlying rating</b>
<b>R. 20</b>	<b>C</b>	This recommendation is fully observed.

## 5. LEGAL PERSONS AND ARRANGEMENTS AND NON-PROFIT ORGANIZATIONS

### 5.1. Legal Persons – Access to Beneficial Ownership and Control Information (R.33)

#### 5.1.1. Description and Analysis

##### *Legal Framework:*

1029. Several different types of legal persons can be established under German law: The limited liability company (*Gesellschaft mit beschränkter Haftung*–GmbH), the stock corporation (*Aktiengesellschaft*–AG), the cooperative (*Genossenschaft*), the foundation (*Stiftungen*), and the registered association (*eingetragener Verein*–e.V.).

1030. The **limited liability company** is formed by one or more founding shareholders adopting the articles of association (*Gesellschaftsvertrag*) and appointing one or several managing directors (*Geschäftsführer*) in a notarial deed (Sections 2 and 3 of the Act on Limited Companies, *Gesetz betreffend Gesellschaften mit beschränkter Haftung*–GmbHG). The minimum capital requirement of a regular limited liability company amounts to EUR 25 000 (USD 34,793). Since November 2008 however, it is possible to form a new sub-category of the limited liability company, the so-called Business Company with Limited Liability (*Unternehmergesellschaft (haftungsbeschränkt)*), which only requires a minimum share capital of one Euro. The traditional corporate structure of the limited liability company provides for only two corporate bodies, the managing directors (*Geschäftsführer*), and the shareholders' meeting (*Gesellschafterversammlung*).

1031. The limited liability company acquires legal personality upon registration in the commercial register. The registration is published by the commercial register electronically. The publication includes the company's firm name, domicile, business purpose, amount of share capital, the date of execution of the articles of association, the identity of the managing directors including their signing authority, the domestic business address of the company, and a list of shareholders. This information is publicly available electronically. Anyone may, therefore, have access to the entries, as well as to their attachments. The entries and notices of the commercial register are an integral part of the business register (*Unternehmensregister*), an internet platform for searching business-related information.

1032. The formation and registration of a **stock corporation** largely follows similar rules. The founding shareholders have to draw up the articles of associations (*Satzung*) in a notarial deed and take over all shares (Section 23 of the Companies Act, *Aktiengesetz*–AktG). The shares can be par-value shares (*Nennbetragsaktien*) or non-par shares (*Stückaktien*) and, independently of this first differentiation, registered shares (*Namensaktien*) or bearer shares (*Inhaberaktien*). The minimum capital requirement amounts to EUR 50 000 (USD 69 585). The rules concerning the required contributions before the application for registration are equivalent to the rules for the limited liability company. The founding shareholders and the members of both constituted boards have to apply for registration of the stock corporation in the commercial register. Instead of a list of shareholders they must attach a list of the members of the supervisory board.

1033. The stock corporation acquires legal personality upon registration, which is also published by the commercial register electronically. The publication includes largely the same information as described above under the limited liability company. In addition to the requirements for limited liability companies, however, shareholders of a stock corporation holding 25% or more, or 50% or more<sup>73</sup> of the shares must notify this to the stock corporation. The company must then publish this information in the company's designated publications, particularly in the Electronic Federal Gazette (*Elektronischer Bundesanzeiger*).<sup>74</sup> If securities, stocks, or bonds emitted by a stock corporation are listed for trading on the capital market, the rules of the German Securities Trading Act (WpHG) impose advanced duties of notification vis-à-vis the shareholders. The significant thresholds amount to 3, 5, 10, 15, 20, 25, 30, 50, and 75% of the shares. Information on these shareholders can be searched electronically by anyone on the BaFin's website<sup>75</sup> and must be disclosed with the business register (see 1048) at the hometown of the shareholders.

1034. A stock corporation may issue either registered or bearer shares. Companies are required to keep a share register but this requirement applies only to corporations that issue their shares in a nominative form. There is no registration requirement when the capital is issued in bearer shares.

1035. An **association** (*Verein*) is a group of persons, established on an indefinite basis, to accomplish a common purpose (examples include sport clubs). The association is represented by a management board. There are associations with and without legal capacity. Legal capacity depends on whether the association's object is to pursue commercial business operations. If this is the case, legal capacity may only be granted by the State, which is rare.<sup>76</sup> An association whose object is not to pursue commercial business operations acquires legal capacity through entry in the register of associations (*Vereinsregister*), i.e. it has a right to be registered if the formal requirements are fulfilled. Sections 57 et seq. of the Civil Code (*Bürgerliches Gesetzbuch* – BGB) establish what the minimum contents of the statutes of an association with legal capacity must be. Section 59 of the Civil Code stipulates that the establishment of the association must be entered in the register of associations, and regulates the content of this entry. Pursuant to Sections 21 and 64 of the Civil Code, the association does not gain legal capacity until the entry has been made in the register of associations.

1036. Registered associations are entered in the register of associations held at the local court located in the same place as the seat of the association. The register of associations is open to public inspection. It contains the name, seat, and management board and the board's power of representation must be entered in the register. There is no requirement to identify the beneficial owners of the association and to enter these details in the register. According to the authorities, such a requirement is not necessary because the individual members of an association do not have the economic ownership of the association's assets and cannot exercise economic control over the association—every member has one vote and any exclusion of voting rights or creation of multiple voting rights must be provided for in the association's articles of agreement, and the original articles as well as any subsequent amendment thereof must be filed with the Register of associations.

1037. A **foundation** (*Stiftung*) is an organization intended to promote on a long-term basis a particular purpose (designated by the founder) through assets dedicated to that purpose. The object of the foundation, stipulated by the founder, can be charitable or the pursuit of private interests. Natural and legal persons

<sup>73</sup> Both thresholds apply conjointly: notification must be made every time either threshold is met.

<sup>74</sup> Which is available online at: [www.ebundesanzeiger.de](http://www.ebundesanzeiger.de).

<sup>75</sup> At <http://ww2.bafin.de/database/AnteileInfo/>

<sup>76</sup> It is rare because the prevailing case law allows the grant of legal capacity to an association pursuing commercial business only if the use of another form of organization (i.e. that of a corporation) would have to be considered unreasonable, which is almost never the case.



may act as founders. Pursuant to Section 81 of the Civil Code, the act of foundation of a foundation with legal capacity must be in writing. Section 80 of the Civil Code provides that the foundation with legal capacity does not come into being until it has been recognized by the competent supervisory authority.

1038. There are both private-law and public foundations. Different legal provisions apply to the creation and activities of private and public foundations. The creation and activities of private foundations are oriented in line with private law, while public law applies to the creation and activities of public foundations.

1039. A private foundation with legal capacity comes into being as a legal entity by virtue of a written act of foundation by the founder and of recognition by the foundation supervision authority. The act of foundation is a unilateral legal transaction by means of which the founding member undertakes to assign assets to fulfil the purpose defined by the founding member, and in which the founding member defines the constitution of the future foundation. Recognition is an administrative act under private law. The foundation is to be recognized if the act of foundation complies with the statutory requirements, the long-term sustained fulfilment of the objectives of the foundation appears to be safeguarded, and the objectives of the foundation do not endanger the public good. Private foundations are subject to the supervision of the foundation authorities of the respective *Land* in which they are headquartered.

1040. A public foundation is a legally-independent administrative organization which was established or recognized by a sovereign state act – by or on the basis of a statute. As part of the public administration, it uses its foundation assets to carry out administrative tasks, and is subject to state supervision. The sovereign act regulates the purpose, assets, and at least the basics of the foundation's constitution and supervision.

1041. A foundation does not have members. It participates in legal transactions via its management board. As mentioned above, the creation of a foundation with legal personality requires recognition by the competent *Land* authority. This authority also monitors compliance with the object of the foundation and the preservation of the foundation assets. According to the authorities, this precondition means that a foundation is not ultimately a suitable tool for ML, unlike foundations or trusts in some foreign countries. The foundations supervisory authority maintains a public directory of the supervised foundations. The directory is open to public inspection. The directory contains the name, legal status, object, bodies, legal representatives, name of the founder (insofar as he or she agrees), date of establishment or termination, and address.

1042. A **cooperative** (*Genossenschaft*) is a member-oriented and a member-controlled organization. The membership basically includes the share of the cooperative, the right in the pro rata deposit and in joint management, as well as the right to use facilities of the cooperative. Additional rights and regulations can be conceded by the articles of the cooperative. The organs of a cooperative are the general assembly of the members, the managing board, and – with exceptions – the supervisory board. An audit by a cooperative auditing association is mandatory every year; for smaller cooperatives, every two years. The cooperative acquires legal personality upon registration, which is published by the cooperative register electronically (Sections 10 to 13 of the Cooperatives Act (*Genossenschaftsgesetz* – GenG).

1043. The cooperative register does not, however, include any information about the identity of the members. The members of the managing board (directors), who have to be members of the cooperative, are to be named in the cooperative register.

1044. Cooperatives must keep a detailed list of their members. The courts may order the disclosure of the list and, if necessary, enforce it by levying administrative fines. Third parties may also consult the list if they have a valid reason for doing so.

1045. According to the authorities, the legal structure of a cooperative makes it factually impossible to obtain control over a cooperative: the cooperative works on the principle of “one man–one vote,” multiple voting rights are highly limited, and in principle, the right to vote must be exercised personally.

***Measures to Prevent Unlawful Use of Legal Persons (c. 33.1):***

1046. The German authorities do not take measures specifically designed at preventing the misuse of legal persons by money launderers or terrorist financiers; they rely on the mechanisms established under the commercial laws and the powers granted to the law enforcement authorities to obtain information on legal entities constituted under German laws:

1047. Stock Corporations may be **listed**, in which case the necessary information will be available to the authorities. According to the authorities, out of some 20 000 stock corporations, only approximately 900 are listed.

1048. For **non-listed companies**, the main sources of information are the various registers, namely:

**Commercial register**

1049. The commercial register (*Handelsregister*) is a public register, which holds the essential details on the legal status of registered companies and merchants, *i.e.* the type of legal entity, the subject of its business activity, its registered offices and, if applicable, the registered capital. The exact content of specific entry in the commercial register depends largely on the type of legal entity to be entered. In all cases, however, the register displays the power of representation of the respective managing partners or directors.

1050. All limited liability companies and stock companies must be entered in the commercial register regardless of the size and nature of their business undertaking, since registration is the condition for their existence from a legal point of view. The shareholders of a limited liability company are not entered into the commercial register itself, but into a list of shareholders that has to be filed with the commercial register and can be inspected by anyone electronically. The shareholders of a stock corporation are not entered into the commercial register itself either, only the founders are; but in case the stock corporation issues registered shares, the shareholders must be entered into the company’s share register.

**Business register**

1051. Additional information on business and bankruptcy disclosures, accounting and financial reports, and capital market information are available at the business register (*Unternehmensregister*). In the case of stock corporations, shareholders who own 3, 5, 10, 15, 20, 25, 30, 50 or 75% of the capital must be disclosed with the business register.

**Register of cooperatives and associations**

1052. The register of cooperatives (*Genossenschaftsregister*) is a public register providing information about the legal status of a registered cooperative (*eingetragene Genossenschaft*, eG).

1053. Pursuant to the Register of Associations Ordinance (*Vereinsregisterverordnung*, VRV), the register of associations (*Vereinsregister*) is maintained at the local courts (with subject-matter jurisdiction).

1054. The purpose of the registers listed above is mainly to establish the structure of the legal entities and the representation rights for commercial law purposes. The information that they contain is, therefore, focused on the entity’s legal status, structure, and purpose; it typically includes the name and address of the

persons who constitute the governing bodies of the legal entities. However, the registers are not really designed to ensure transparency on the control and beneficial ownership of the legal entities in a way which would be useful in the fight against ML and TF. In order to identify those who ultimately own and control a specific legal entity, the authorities must, therefore, rely on alternative channels of information, such as the following.

1055. In many instances, the registration is requested through the intermediary of a notary. As described in Section 4.1 above, notaries are subject to the CDD requirements set out in the AML Act, and must identify their customer and the beneficial owner of the legal entity to be established and maintain that information. The notaries must make the information about the legal entity available to the authorities upon request. However, the information that the notaries maintain is usually that which was provided at the time of registration and is not kept up-to-date. It may, therefore, not always be relevant. Moreover, not only is there no general obligation to request the registration through a notary, but even in cases in which a notary was involved in the registration process, the mention of his or her name is not necessarily always contained in the register itself. In these circumstances, the competent authorities may not always know which notary to turn to, and when they do, the information that the notary provides may no longer be of any use.

1056. Stock corporations that issue their capital in nominative form are required to keep a share register; they must, therefore, keep a record of who the shareholders are. The register is not public but may be accessed by law enforcement agencies if necessary. Registration is not mandatory but, in principle the assertion of shareholder rights requires registration in the share register, even though it is possible to act by proxy. The registered holders of shares are required by law to provide the stock corporation with all information necessary to keep an accurate share register. A person registered in the share register as the holder of registered shares must notify the issuer upon request to which extent the shares belong to him or her or on whose behalf he or she holds the shares. In the absence of such a request, there is no indication of the real beneficial owner of the shares. Moreover, it is unclear whether and to what extent corporations seek the identity of the beneficial owners of other legal entities that may own some of their shares. There is no registration obligation when the capital is issued in bearer form (see description below).

1057. Finally, in the case of foundations, in particular the private foundation, no information is readily accessible.

***Access to Information on Beneficial Owners of Legal Persons (c. 33.2):***

1058. As mentioned above, a certain amount of information on all types of legal entities except foundations is available at various publicly-accessible registers. However, the information entered into the registers does not necessarily include information on the beneficial ownership of the legal persons and may only, in certain circumstances, provide the authorities with some direction as to where some further information, such as information on the beneficial owners, may be found. These measures do not guarantee that the information that may be obtained is adequate for AML/CFT purposes, accurate and current. Considering that the authorities must take additional steps before having access to that information, it is unlikely that they may do so in a timely fashion. Access to information on the beneficial owners may prove arduous, in particular in the case of stock corporations that are not listed and that have issued their shares in bearer form, as well as in the case of a private foundations.

***Prevention of Misuse of Bearer Shares (c. 33.3):***

1059. Stock corporations may choose to issue their shares either in nominative or bearer form. They cannot, however, mix the two forms – the entire capital is, therefore, issued in one form or the other.

1060. As mentioned above, there is no obligation to keep a register of bearer shares and shareholders are not obliged to inform the company of the purchase or sale of shares. There are, therefore, no guarantees that the management of the company knows its shareholders—but there are duties of notification as described above (33.1). If a shareholder wants to exercise his shareholder's rights, *e.g.* the right to take part in the shareholder's meeting or the right to dividends, he or she must legitimize himself by proving possession of the bearer shares in order to enable the management to take cognizance of the identity of the shareholder. Pursuant to Section 123(1), first sentence, of the Stock Corporation Act (*Aktiengesetz*, AktG), the statutes of a stock corporation will determine how the entitlement to attend a meeting of shareholders or to exercise voting rights is to be proven for holders of bearer shares. In practical terms, this is often implemented by the shares having to be lodged with the company. The person lodging the shares consequently becomes known to the stock corporation. In the case of companies listed on the stock exchange, it is sufficient to have the financial institution managing the portfolio issue proof in text form as to the shareholding in accordance with the stipulations of Section 123(3), second sentence, of the Stock Corporation Act. The financial institutions managing the portfolio are subject to the obligations set out in the AML Act, and must, therefore, identify the shareholder when the portfolio is opened. In case of a dividend payout, the banking information of the holder of the shares must be provided to the company.

1061. According to the authorities, the problem of not knowing the shareholder's identity is not that serious in practical terms because individual certificates are not frequently used. Nearly all shares of publicly-listed stock companies are certified in global notes. The right of the shareholder to the issue of a certificate for his share may be restricted or excluded so that all shares are certified in a global document (Section 10 (5) of the Stock Corporation Act). This provision was implemented in 1998. Since then, due to cost savings aspects, the issue of a global document instead of individual share certificates has become common practice with listed companies. Moreover, the financial institution managing the portfolio is subject to the obligations set out in the AML Act, regardless of whether the securities in its deposit are certified individually or globally. Exact number of companies that issue either global notes or individual share is, however, not available and the extent of the practice described is not established.

1062. The authorities maintain that the intangible individual shares are registered in safe deposits by the custodian banks, who know the depositor and consequently the shareholder, and public prosecutors may access this information. This reflects, however, only part of the practice and there is no legal requirement to deposit shares. The authorities mentioned further that companies that are not publicly-listed stock companies (of which there are about 19 000 in Germany) typically emit registered shares; the company, therefore, has a share register and knows its shareholders. The estimated number of not publicly listed stock companies issuing bearer shares lies between 1 000 and 2 000. Exact figures are not available, and the authorities did not assess the risk of ML and TF posed by companies that issue bearer shares.

***Additional Element – Access to Information on Beneficial Owners of Legal Persons by Financial Institutions) (c. 33.4):***

1063. Financial institutions face the same limitations as the authorities when trying to access beneficial ownership information of legal persons.

***5.1.2. Recommendations and Comments***

1064. The scope of information available varies greatly according to the type of legal entity: at one end of the spectrum, information is available on all shareholders of the limited liability companies, while at the other end of the spectrum, very little to no information is disclosed in the case of private foundations and stock corporations that are not publicly listed and that issued their shares in bearer form. However, in all these cases, the information does not focus on the control and beneficial ownership of the entities in the sense of the standard. The current mechanisms in place do not guarantee that the competent authorities

have access in a timely fashion to adequate, accurate, and current information on the control and beneficial ownership of legal entities.

1065. Information on foundations, in particular private foundations, is close to nonexistent. Furthermore, the fact that stock corporations may issue the entirety of their capital in bearer shares entails that, as far as these companies are concerned, the identification of their beneficial owners is virtually impossible. These two elements alone create a potentially considerable risk of ML and TF.

1066. In order to comply fully with Recommendation 33, Germany should:

- Ensure that beneficial ownership on all types of legal entities is made accessible to the competent authorities.
- Assess the risk of ML and TF posed by non-publicly listed companies that issue bearer shares and take necessary measures to mitigate the risk.

### 5.1.3. Compliance with Recommendations 33

	Rating	factors underlying rating
R.33	NC	<ul style="list-style-type: none"> <li>• No mechanisms in place to ensure in all cases access in a timely fashion to information on the control and beneficial ownership of legal entities other than publicly-listed stock corporations.</li> <li>• Lack of transparency over non-publicly listed stock corporations that issue their shares in bearer form, and over private foundations.</li> <li>• No risk assessment undertaken by the authorities to ascertain the risk of ML/TF in the case of joint stock companies which have issued bearer shares.</li> </ul>

## 5.2. Legal Arrangements — Access to Beneficial Ownership and Control Information (R.34)

### 5.2.1. Description and Analysis

#### Legal Framework:

1067. Germany has legal arrangements similar to the Anglo-Saxon express trust, namely, the foundation (*Stiftung*; described above under Recommendation 33) and the *Treuhand*, also referred to as *Treuhandverhältnisse*. The terms “*Treuhand*” and “*Treuhandverhältnis*” are used in a variety of contexts, and their definition may vary in scope depending on the particular circumstances of each *Treuhand*.

1068. In a broad sense, the *Treuhand*, or “*Treuhandverhältnis*,” is a contractual relationship by which one party, the *Treugeber*, requires another, the *Treuhänder*, to manage his or her assets in a certain way. It is a contract which is not regulated in law, but is based on the general principle of the autonomy of the contracting parties and delimited by jurisprudence and doctrine. The *Treuhand* can exist without any written record. It can be concluded between any two persons capable of being party to a contract. It is created when the *Treuhänder* is authorized to exercise rights over property in his or her own name, on the basis of and in accordance with a binding agreement with the *Treugeber*. It may involve third party beneficiaries but is most often a two-party relationship. It may also take different forms: it may be hidden (*verdeckte Treuhand*) or disclosed to third parties (*offene Treuhand*); the *Treuhänder* may be authorized to

manage the assets under the *Treuhand* (*das Treugut*) in the interest of a third party (*fremdnützige Treuhand*) or in his or her own interest (*eigennützigen Treuhand*).

1069. In a narrower sense, a *Treuhand* relationship is deemed to be given only for relationships entailing the performance of obligations in which the *Treugeber* (trustor) enters into an agreement to transfer the objects or rights to the *Treuhänder* (trustee), and the latter agrees to hold and administer them in the interest of the *Treugeber*. It is sometimes translated into English as a fiduciary trust relationship.

1070. In addition, the term *Treuhandverhältnis* is also used as an umbrella term for a large number of legal relationships entailing an obligation on a person (the *Treuhänder*) to assert certain rights (*Treugut*) in the interest of another person (beneficiary–*Treugeber*) or of a third party. Such a relationship can be founded by a statute or by a legal relationship while the term “fiduciary trust relationship” only covers trust relationships founded through a legal transaction.

1071. When the *Treugeber* and the *Treuhänder* agree that the *Treuhänder* is to assert certain rights in the interest of the *Treugeber*, and if the *Treuhänder* acts on a not-for-profit basis, this constitutes a mandate in accordance with Section 662 of the Civil Code; if the *Treuhänder* receives a fee, this constitutes a business management contract in accordance with Section 675 of the Civil Code.

1072. So that the *Treuhänder* can dispose of the property, the *Treugeber* may assign the *Treugut* to him or her, may for instance grant to him or her ownership of an item, or may grant to the *Treuhänder* the necessary legal power, for instance empowerment (enabling *Treuhand*) or proxy (proxy *Treuhand*) so that he or she can dispose of the trust property. In the case of a proxy *Treuhand*, the *Treuhänder* must always disclose to third parties that he or she acts for the *Treugeber* when disposing of the *Treugut*. In accordance with Section 164 of the Civil Code, the *Treuhänder* may only effectively act as the representative of the *Treugeber* if he or she acts not only with the proxy of the *Treugeber*, but also on his or her behalf (so-called principle of common knowledge).

1073. *Treuhandverhältnisse* in legal transactions largely serve two purposes:

- Security purposes (security *Treuhand*). Or
- Administrative purposes (administrative *Treuhand*).

1074. With a for-profit security *Treuhand*, the *Treugeber* undertakes to transfer a right, for instance the ownership of a moveable item, to the *Treuhänder* to secure a claim of the *Treuhänder* towards the *Treugeber*. If the *Treugeber* does not satisfy the claim, the *Treuhänder* may exploit the article. If the *Treugeber* has satisfied the claim, the *Treuhänder* is obliged to transfer ownership of the item back to the *Treugeber*.

1075. An administrative *Treuhand* is established in the interest of the *Treugeber* (trustor) or of a third party. There may be a wide variety of reasons for such administrative *Treuhand*. As a rule, a *Treuhänder* is commissioned because he or she is better able to administrate the property than the *Treugeber* or the third party. A special case occurs if the administration of the property requires special expertise or if the property is to be administrated on behalf of a third party who is personally unable to do so, for instance by reason of being a minor.

1076. Although no precise figures exist on the subject, the *Treuhand* is a very common feature of the German economy (as it is, in some form or another, in other common law jurisdictions). Lawyers, notaries, and other TSPs often act as *Treuhänder*, but any member of the general public who can be party to a contract can also act as *Treuhänder*.



1077. Overall, the German *Treuhand* is similar to the Anglo-Saxon express trust in some ways, but it does not have effects *in rem* comparable to those of a trust. *Treuhand* relationships, therefore, do not grant the same degree of protection as the Anglo-Saxon trust does. All dispositions by the *Treuhänder* regarding the property transferred to him are effective, even if he were to act in bad faith and contrary to the contractual arrangements made. Like the trust, however, it may offer relative anonymity of the beneficial owner of the *Treugut*. It may, therefore, be misused for ML and TF purposes to the same extent as the Anglo-Saxon trust. The extent of this risk has not been assessed by the German authorities.

1078. The *fideicomiso* and the Anglo-Saxon trusts cannot be established under German law.

***Measures to Prevent Unlawful Use of Legal Arrangements (c. 34.1):***

1079. No measures have been implemented to prevent the unlawful use of *Treuhand*, other than the obligations for disclosure mentioned below.

***Access to Information on Beneficial Owners of Legal Arrangements (c. 34.2):***

1080. There are no measures in place to ensure in all instances access to the information on the beneficial owners of a *Treuhand* and there is in particular no registration of *Treuhandverhältnisse* or of *Treuhänder*. According to the authorities, such a registration requirement would not be practicable due to the everyday character of many *Treuhandverhältnisse* (examples include selling something on behalf of a friend). It is, therefore, impossible to determine how many *Treuhand* are established in Germany, the amount of property that they cover, and who the *Treuhänder* are. There are, however, a few instances where the disclosure of the *Treuhand* and its parties is requested by various laws:

- a. The relationship must be disclosed in certain circumstances, in particular when opening a bank account: pursuant to Section 4(5) of the ML Act, the customer must disclose on whose behalf he or she is acting. Other circumstances include the following:
- b. As a legal relationship under the law of obligations, a *Treuhand* based on a legal transaction in principle gives rise only to rights and duties for the contracting parties, that is, the *Treugeber* and the *Treuhänder*, and *Treuhänder* possibly to rights for a beneficiary third party. Insofar as rights towards other third parties are claimed on the basis of the *Treuhand*, this always requires the *Treuhand* to be disclosed.

1081. Lawyers and notaries who have agreed *Treuhandverhältnis* with their clients may for instance open fiduciary accounts and deposits with banks in order to keep *Treuhand* property there for one or more clients. The financial institution holding the account is to be informed, at least in response to its enquiry, of the party on whose behalf the fiduciary account is being held. If a fiduciary account has been effectively established, the bank may only access the fiduciary account in respect of claims against the trustee insofar as these claims have arisen with regard to the trust account itself.

1082. Should the *Treuhänder* become insolvent or coercive execution measures on the part of private creditors are effected with regard to the property, special rights for the *Treugeber* ensure from the trustee relationship which prevent the property being exploited by the insolvency administrator or the private creditors of the *Treuhänder*. However, these rights can only be asserted if the *Treugeber* discloses the *Treuhand* and can prove that there is a *Treuhand* in the event of a dispute.

1083. Additionally, as well as the obligations in accordance with the AML Act, there are other obligations under public law which may contribute towards the disclosure of *Treuhand*. For instance, the *Treugeber* may be obliged to state a *Treuhand* in his or her tax declaration if this is relevant in terms of

fiscal law because income or expenditure resulting from the administration of the trust property are to be included in his or her tax assessment.

1084. Access to information pertaining to *Treuhands* may be also obtained through law enforcement powers. However, the absence of registration greatly inhibits the implementation of these powers.

1085. In conclusion, the disclosure of the information concerning the existence of the *Treuhand* and the parties to it is limited to specific circumstances. In the absence of central registration, the authorities are hard pressed to establish the presence of a *Treuhand*, let alone establish the identity of its beneficial owner.

***Additional Element – Access to Information on Beneficial Owners of Legal Arrangements by Financial Institutions) (c. 34.3):***

1086. As mentioned above, a *Treuhänder* must inform financial institutions that he or she is acting on behalf of someone else and provide the identity of that person.

**5.2.2. Recommendations and Comments**

1087. While there are some obligations to disclose the *Treuhandverhältnis* in place, these measures are not sufficient to mitigate the risk of misuse of *Treuhandverhältnisse*.

1088. In order to comply fully with Recommendation 34, Germany should:

- Enhance transparency over *Treuhands*.

**5.2.3. Compliance with Recommendations 34**

	Rating	Summary of factors underlying rating
R. 34	NC	<ul style="list-style-type: none"> <li>• Insufficient measures in place to ensure transparency over <i>Treuhand</i>.</li> </ul>

**5.3. Non-Profit Organizations (SR.VIII)**

**5.3.1. Description and Analysis**

***Legal Framework***

1089. In light of the socially valuable work performed by non-profit organizations and the responsibility they have generally exercised within the law, the German government is of the view that the non-profit sector should not be unreasonably burdened by bureaucratic or legal obstacles. Consequently, Germany has chosen not to adopt a statutory supervisory framework and a formal monitoring regime for the entire NPO sector specifically for purposes of combating terrorism. Rather, the authorities have adopted a two-prong approach which relies on measures to ensure the transparency of the sector and targeted, intelligence driven monitoring, surveillance, investigation and suppression of extremists and terrorist activities, including financial support of terrorism.

1090. Transparency arrangements include a “Donation Seal” program (discussed below) which covers the larger NPOs and certifies those NPOs that, on a voluntary basis, subscribe to high standards of transparency and accountability. The program also spotlights NPOs that do not adhere to such standards. Transparency arrangements include outreach programs to raise awareness and sensitize the NPO sector to

the risks of being abused for ML. Outreach extends to the financial sector to raise its awareness of the vulnerabilities to TF of transactions involving the NPO sector.

1091. In Germany, it is primarily a tax issue whether an organization is considered “non-profit” (*gemeinnützig*) or not. Organizations have to apply for a notice of exemption with the tax authority in order to qualify for tax relief based on their non-profit status. Qualification for non-profit status is based on the benevolent, social, ecclesiastical, or non-profit objectives of the organization. The legal form the organization chooses has no bearing on the issue of non-profit status. Once an organization has been granted non-profit status, the fiscal authorities may inspect the accounts of any NPO and oversee how funds are appropriated.

1092. NPOs are required to provide annual audits of funds collected, including the intended purpose of the funds and the uses to which the funds were applied (the organization is not allowed to act on its own behalf; it shall not pursue goals primarily serving its own economic interest).

1093. Tax authorities may carry out tax investigations as warranted. In practice such investigations are exceptional and normally triggered on the basis of independent evidence of problems, including reports from security services.

1094. As mentioned above, the legal form the organization chooses has no bearing on the issue of non-profit status. In addition to incorporated and unincorporated associations, foundations and corporations, stock corporations (AG) and German limited liability companies (GmbH), cooperative societies and enterprises of an individual or commercial nature, and corporations under public law may claim tax privileges if they hold non-profit status. Based on a determination of NPO status, tax benefits have been granted to between 400 000 and 500 000 associations (*Vereine*) and approximately 18 000 foundations (*Stiftungen*).

1095. While there is no specific regulation of the NPO sector, in order to qualify for favorable tax treatment, NPOs are subject to registration and reporting obligations depending on their legal form.<sup>77</sup> Additionally, there are numerous transparency measures and arrangements provided by NPOs in a self-regulating manner.

1096. Based on a study by the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth (BMFSFJ) in 2006, the annual volume of donations in Germany fluctuates between EUR 2.6 billion and EUR 7 billion (USD 3.6 billion and USD 9.7 billion). Among other things, donating behavior is dependent on the occurrence of major catastrophes, such as natural disasters, which prompt public donations. Therefore, the average volume of donations in Germany annually lies in the range EUR 3-EUR 5 billion (USD 4.2-7.0 billion).

1097. In recent years, cash donations have increasingly been replaced by wire transfers or pledge programs. Today, cash donations are collected in only a few limited contexts, for example by religious institutions (churches, mosques) or in certain cases on the street or door-to-door. Receipts may be issued for tax-deductible cash donations and, when filed, provide the revenue administration with a means to verify that the donation was used for the specified purpose.

---

<sup>77</sup> See Interpretative Note to Special Recommendation VIII, 6, b (iii) “Specific licensing or registration requirements for counter terrorist financing purposes are not necessary. For example, in some countries, NPOs are already registered with tax authorities and monitored in the context of qualifying for favorable tax treatment (such as tax credits or tax exemptions).

1098. Noncash donations made to a non-profit organization which are transferred to ultimate beneficiaries through licensed financial institutions can generally be monitored through the interface of the bank account and traced in criminal investigations.

***Review of Adequacy of Laws & Regulations of NPOs (c. VIII.1):***

1099. c. VIII.1.i – Review of the NPO sector. In 2003, Germany undertook a review of the legal and regulatory structure and the operational activities of its NPO sector, focusing on the sector’s vulnerability to abuse for TF purposes. The September 2003 report of that review, “German Report on the Non-Profit Sector,” was subsequently amplified and submitted to the FATF Working Group on Terrorist Financing on August 31, 2004 as WGTF/58. The WGTF document reviews the NPO situation in Germany, discusses the relevant legal framework, and enumerates several suggestions for improvements to prevent abuse of the sector for TF purposes.

1100. The authorities state that the adequacy of laws and regulations relating to NPOs remains under review and their approach has and continues to be that, where a need is recognized, adjustments have been made; the examples below serve to illustrate this approach. More concretely, pursuant to legislation dated December 4, 2001, the application of the Act Governing Private Associations (VereinsG) was extended to extremist religious organizations and ideological associations, making it possible for the first time to prohibit such associations and their activities. Prior to this, official investigations had revealed that a recognized non-profit organization had been pursuing extremist objectives under the guise of a religious community.

1101. In addition to the new legislation noted above, the fiscal code has provisions for the denial of NPO status to associations involved in terrorist activities or contradicting the notion of international understanding, and requiring reporting of such activities to the Constitutional Protection Agency and filing an STR. These provisions are in Section 51 (3) of the Fiscal Code. To be eligible for a tax benefit, the articles of association and the actual management of an association must preclude it from pursuing terrorist efforts or activities that contradict the notion of international understanding. These conditions are derived from Section 4 of the Act Regulating the Co-operation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution (*Bundesverfassungsschutzgesetz*, BVerfSchG). To the extent any doubt as to whether the requirements for recognition are satisfied, such doubt operates to the detriment of the organization, *i.e.* no tax privileges will be granted. The tax authority informs the constitutional protection agency (the competent domestic intelligence service) of any findings made in its tax proceedings substantiating a suspicion of efforts within the meaning of Section 4 of the BVerfSchG – specifically, the support of terrorist activities. Pursuant to Section 31 b of the Fiscal Code, the tax authorities are also required to promptly notify the competent law enforcement agencies and send a copy of such notice to the FIU of any information suggesting that TF within the meaning of Section 1 (2) of the Money Laundering Act has been or will be committed or attempted.

1102. Additionally, for associations which violate criminal law or contradict the constitutional order or the notion of international understanding, the Act Governing Private Associations allows for prohibition of such associations pursuant to which the organization’s entire assets will be confiscated. The benefits unlawfully received must be reimbursed. If the relevant requirements are met, the representatives of the relevant organization will be subject to criminal liability. If recognition of the organization as a non-profit organization was fraudulently obtained because the prerequisites for recognition were not met, liability may arise pursuant to Section 370 of the Fiscal Code based on tax evasion. The attempt is punishable pursuant to Section 370 (2) of the Fiscal Code. In the event of negligent conduct, the statutory representative would be committing an administrative offense pursuant to Section 378 of the Fiscal Code, which is punishable by a fine of up to EUR 50 000 (USD 69 585). This does not affect the prosecution of

the parties involved in the organization pursuant to the criminal provisions of Sections 129 a, 129 b of the CC pertaining to TF.

1103. On August 31, 2002, using authority under the amended Act Regulating Public Associations, the registered, nationwide foreigners' association, AL-AQSA e.V. was banned and dissolved and its assets confiscated and forfeited. The decision was taken on the basis that: (1) the activities carried out by AL-AQSA e.V. support, advocate, or are intended to bring about, the use of force as a means for enforcing political, religious or other interests; and (2) AL-AQSA e.V. supports an association outside the Federal Republic which advocates and initiates attacks on persons or property. Yatim-Kinderhilfe e.V., which intended to continue the activities in collecting funds, was banned and its assets confiscated on September 5, 2005.

1104. c. VIII.1.ii – Documentation (articles of association, names and addresses of the members of the management board) on all associations entered in the Register of Associations is available at the Local Courts. Registers of associations are public, *i.e.* they may be inspected by anyone. Registers of associations are maintained electronically and are accessible on line. Websites have been developed by regional governments linking the various websites to the registers of the individual *Länder*. Although the information is available to the public on the web, a fee is charged. Additional transparency and public oversight might be achieved by eliminating the fee for access. In addition, the Federal Office of Administration (BVA) maintains a central register for associations of aliens pursuant to the Act Governing Private Associations (in which associations of aliens without legal personality must also be registered). The tax authorities have documentation on all non-profit organizations in Germany with respect to financial statements, financing sources and recipients. For information on DZI, see above. Pursuant to Section 31 b of the Fiscal Code, the tax authorities are required to promptly notify the competent law enforcement agencies and send a copy of such notice to the FIU of any information suggesting that TF within the meaning of Section 1 (2) of the Money Laundering Act has been or will be committed or attempted by any person or, for example, also any (non-profit) organization.

1105. Based on intelligence information, the authorities make use of available sources of information to analyze the likelihood of financing of terrorism and to identify and preclude terrorist activity. Such risk assessments extend across multiple sectors and activities, including but not limited to the NPO sector. Available information may not always be timely because of outdated baseline data, limited requirements to submit updated information, and infrequent compliance monitoring.

1106. c. VIII.1.iii – Federal and state security authorities continue to evaluate current trends in TF, including TF by non-profit organizations. The findings and evaluations are incorporated into the situation reports (SITREP) on TF. Current trends are also included in the FIU newsletter, which is provided to the institutions and persons covered by the Money Laundering Act. Based on intelligence information, the authorities recalibrate the entities and sectors that are targeted for surveillance for terrorist activity and financing of terrorism. In addition, risk assessments provided by the FIU and intelligence authorities provide more general orientation to surveillance activities.

***Outreach to the NPO Sector to Protect it from Terrorist Financing Abuse (c. VIII.2):***

1107. c. VIII.2. i. – Outreach to raise awareness in the NPO sector about the risks of terrorist abuse and the availability of measures to protect against such abuse was particularly active in 2002 around the time the International Best Practices paper was being prepared and issued. Following that, a roundtable was created with representatives of major non-profit associations in Germany in which the Federal Ministry of the Interior and the Federal Ministry of Finance participated. The roundtable provides a forum to present current findings and evaluations, to sensitize NPOs to the concerns of the security authorities, and to raise



awareness of what associations themselves can do to prevent abuse of NPOs. The roundtable continues to meet on an occasional basis.

1108. Beyond the roundtable, there has been only limited organized awareness raising with regard to misuse of NPOs for TF purposes. DZI conducts an annual workshop with all donor seal organizations which include topics such as anti-corruption, but TF has not been a specific focus of the workshops. Nor does DZI have a public relations section to propagate information on key issues. Other organizations that are potential forums for awareness raising about TF, such as the German Association of Foundations and the German Federation of Welfare Organizations, do not appear to have active programs. The German Association of Foundations has, however, published in 2006 some “*Guiding Principles of Good Practice for Foundations*,” also posted on the internet.<sup>78</sup> They are intended in particular to sharpen awareness on the part of all persons concerned with regard to avoiding potential conflicts of interest, ensuring adequate transparency in the conduct of foundation affairs, and ensuring that foundation funds are allocated efficiently. Foundations can declare these principles as mandatory which is a means to impose pressure among foundations. Furthermore, public discussion on transparency of the NPO sector becomes more frequent. The authorities see the need to balance general awareness efforts with the risk of undermining public confidence in the social function of NPOs. As noted, they believe a more targeted, intelligence-driven approach is a more effective means of achieving the twin goals of combating terrorism and maintaining public confidence in the NPO sector.

1109. c. VIII.2.ii – Under the DZI Donation Seal initiative, programs have been developed for major NPOs to commit to integrity standards of transparency and accountability designed to foster public confidence in the administration and management of NPOs. Adherence to such standards is assessed by DZI and forms the basis for award of Donation Seals. In addition, DZI makes the public aware of major NPOs that do not qualify for the Donation Seal.

***Supervision or Monitoring of NPOs that Account for Significant Share of the Sector’s Resources or International Activities (c. VIII.3):***

1110. c. VIII.3. Monitoring the fundraising market and fundraising organizations is the function of the German Central Institute for Social Issues (DZI). DZI is an independent private law foundation sponsored by the Berlin Senate, the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth, the German Chamber of Industry and Commerce, the German Association of Cities and the Federal Association of Non-statutory Welfare. A primary objective of DZI is to promote transparency, to provide information and an assessment of NPOs, and to warn against nontransparent and dubious fund raising organizations. According to DZI, of the multitude of NPOs, only about 3 000 solicit donations on a regular, systematic, and national basis. The survey covers both the domestic and international activities of the largest NPOs active in Germany. The DZI awards the German “Donation Seal” (*Spendensiegel*) to organizations that promote transparency and agree to comply with broader rules of supervision and review by DZI. DZI publishes an annual fund raising guide, the DZI Donation Almanac. In addition to awarding its seal, the DZI also offers advice to donors on approximately 350 organizations which solicit donations nationally but do not have its seal. A database is being developed to provide, based on voluntary disclosures, information on the objectives, subject matter, and activities of all non-profit organizations. While partly sponsored by official organizations, DZI operates on a voluntary basis and has no enforcement authority

1111. The DZI initiative focuses on the approximately 3 000 NPOs that account for a significant portion of the financial resources under control of the sector (that is to say the preponderance of the donation funds solicited on a regular, systematic, and national basis). These organizations account for

<sup>78</sup>

[www.Stiftungen.org](http://www.Stiftungen.org).



approximately half of all German charitable donations (among these all big donation soliciting organizations) and a substantial share of the sector's international activities.

1112. c. VIII.3.1 – Information on the purpose and objectives of their stated activities is required to be filed both with the tax authorities for purposes of qualifying for tax benefits and with the register of associations (or the register of companies, or register of foundations) to establish legal personality. Names and addresses of board members must also be filed. Registration information is available to the public, either on-line or at the local courts. Basic information on tax benefit organizations is also available from the tax office.

1113. Examination of the accounts and organization and objectives of an NPO takes place primarily at the time of application for NPO status. Tax exemption status must be renewed annually, including an updating and review of the purposes and governance of the NPO. NPOs have to regularly file a tax return. With each tax return, the fiscal authorities check if the organization still complies with the requirements for the favorable tax treatment of an NPO (Sections 51 and following AO). Failure to file required reports may lead to withdrawal of tax benefits.

1114. The tax authority does not solely check what is stated in the articles of the association, but also the actual management of the organization. The organization has to prove that its actual management complies with the legal prerequisites by submitting detailed breakdowns of incomes and expenditures. Furthermore, the donation receipts' rightfulness will be checked in order to ensure that all funds are fully accounted for and are spent in a manner that is consistent with the purpose and objectives of the organization's stated activities.

1115. In Germany, tax information is not open to the public. The public will find registration data for associations and other legal entities from the registrar, which is frequently maintained on-line.

1116. c. VIII. — 3.2 Although freedom of association is a fundamental right protected under Article 9 of the German Basic Law, Article 9(2) provides that associations whose aims or activities contravene criminal law or are directed against the constitutional order or the notion of international understanding shall be banned. In keeping with these constitutional provisions, the Act Governing Private Associations contains provisions applicable to all associations, pursuant to which action may be taken against associations that abuse the freedom of association. Section 3 of the Act has provisions that allow the prohibition of an association itself or of certain of its activities; a ban as a general rule extends to seizure and confiscation of assets; violations are subject to sanction. The Act also grants special investigative powers to the agencies enforcing the prohibition which are flanked by the general powers of the security authorities where actual indications of TF exist. The authority imposing the ban is: (a) at the *Land* level, the Supreme *Land* Authority or the authority responsible for associations, or (b) at the Federal level, the Federal Minister of Interior. In the period since the Act was first adopted in December 1966, the authority to ban associations has been exercised on numerous occasions, for a variety of offenses. During that period, *Länder* have banned some 72 associations and the BMI has banned an additional 36.

1117. In cases where an association is banned, there is also authority to seize and confiscate assets. As noted, the grounds for prohibition, among other things, include dangerous influence on public safety and order and support of terrorist organizations. The powers available for prohibition and seizure and confiscation have been used in at least two cases related to terrorism. The prohibition authority has been used numerous times for various causes. Enforcement actions under this Act do not preclude prosecution for related civil or criminal offenses. Failure to comply with tax violations can lead to withdrawal of tax benefits.

1118. c. VIII. 3.3 – As described under the legal framework, NPOs are required to apply to the tax authorities in order to be eligible for tax benefits and (hence) NPO status. A condition of receiving tax benefits is establishing legal personality, which requires registration as an association or as a foundation or as some other form of legal entity. Licensing is not required. Tax filing information is available to the competent authorities, as is association, foundation, and corporate registration information.

1119. Most NPOs tend to choose the legal form of an association (*Verein*). This is defined as a permanent association of a larger number of persons to achieve a common purpose which is organized as a body corporate pursuant to its articles of association, operates under a common name and is designed to have a fluctuating membership (Section 21 and following of the Civil Code (*Bürgerliches Gesetzbuch*, BGB). The constitution and structure of an association are determined by the articles of association it itself adopts, for which there are no formal requirements. As a result, associations have wide autonomy and discretion in their operations and activities.

1120. In order to obtain legal personality (and the various rights that provides, e.g. contracting, access to tax and subsidy benefits, authorization for fund raising, etc.), an association must be entered in the Register of Associations. Registration requires submission of the association's charter and the names of the association's management board. Registers are maintained at the *Länder* level by the Local Courts.

1121. Associations are governed by the Act Governing Private Associations (*Gesetz zur Regelung de öffentlichen Vereinsrechts* (VereinsG). Groups who have not achieved legal personality through registration are also subject to the act. Specifically, where several persons voluntarily unite over a longer period of time for a common purpose and defer their individual will to an organized decision-making process, for example, to pursue social or charitable objectives, they are governed by the Act. Separate provisions of the Act concern associations whose members are all or, to a large majority, third-country nationals (*Auslanderverein*) or have their domicile abroad. These associations have a general duty to register which requires that additional information be provided as to the countries in which the association has sub-organizations.

1122. Stock corporations and limited liability companies are subject to the German Commercial Code (*Handelsgesetzbuch*, HGB) and connected laws requiring publication of annual accounts with the register at the Local Courts.

1123. Foundations are a further legal form of organization in which NPOs can be organized. An independent foundation constituted under civil law is a private law entity; it is regulated by the German Civil Code, BGB (Sections 80 and following), and the foundation laws of the *Länder*. A so-called foundation business agreement, which is needed to establish a foundation, must receive state approval. A foundation is subject to statutory state monitoring via the foundation supervisory authority, which ensures that state laws are upheld. The foundation is obliged to provide the supervisory authority with an annual report (annual balance of accounts with an income and expenditure report, as well as a written report on the fulfillment of the foundation aim, must be issued). The foundation's Board of Directors must store all financial records for a period of ten years and all correspondence for a period of six years. Certain decisions require the involvement of the foundation supervisory authorities (obligation of disclosure, authorization). The foundation supervisory authority's power to intervene extends from the dismissal of Board members to the dissolution of the foundation or the alteration of its purpose, should the foundation not be in the position to meet its aims, or its status as an organization serving the public good is in jeopardy. The *Länder* foundation laws also incorporate a legal requirement, in which foundation supervisory authorities are obliged to publish their foundation directories online.

1124. c. VIII. 3.4 – The German Fiscal code (*Abgabenordnung*, AO) stipulates in para. 147: “The following documents shall be stored for a period of ten years for tax reasons: accounts and records,

inventories, annual reports, situation reports, the opening balance sheet as well as the operating instructions and other organizational documents needed for their comprehension as well as records of domestic and international transactions. Other documents (such as relevant correspondence) to the extent that these are of relevance for taxation shall be stored for six years.” For NPOs, such records include records of how funds have been raised and how they have been spent. The record-keeping requirements do not require that domestic and international transactions be separately identified.

1125. Further record-keeping retention rules under registration legislation can be found in the German Commercial Code (*Handelsgesetzbuch, HGB*): Section 257 regulates that every merchant and company has to keep records for six years; financial statements and some other particular documents have to be kept for ten years. These documents may also be used as a proof in criminal procedures (in cases of TF) and can be confiscated by police and public prosecutors according to the CPC.

1126. c. VIII. 4.1 – The Joint Counter-Terrorism Center Task Force (GTAZ) is the principal entity for coordinating and sharing information about terrorism and TF. The GTAZ was established in Berlin, Germany in 2004. GTAZ houses approximately 220 specialists from the police (including the Customs Criminological Office (ZKA)), intelligence services, the Public Prosecutor General at the Federal Court of Justice (GBA), and the Federal Office for Migration and Refugees (BAMF) working together to conduct, *inter alia*, background analyses and intelligence support analyses in the area of Islamist terrorism. Some 40 intelligence and investigating bodies coordinate under the auspices of the GTAZ. In appropriate cases, specialists from the financial supervisory authority, as well as foreign experts may be brought in. (See discussion under Recommendation 27 for additional background on the role and activities of the GTAZ). Information held by BKA is available to law enforcement agencies and BKA has published on its website notices regarding TF developments.

1127. c. VIII.4.2. – Registration information is available to law enforcement as well as to the public. Information collected by the fiscal authorities for purposes of the granting of tax benefits, including financial and programmatic information, can be made available to law investigators under appropriate authority. Under its regulatory investigatory powers, law enforcement may carry out investigations of NPOs, *i.e.* when there is the suspicion that an NPO has committed tax evasion (Sections 370 and 402 German Fiscal Code (*Abgabenordnung, AO*) which refer to the CPC. Regulatory investigatory powers include confiscation (Sections 94 and following StPO) and search (Sections 102 and following StPO).

1128. c.VIII.4.3 – As discussed above, the GTAZ is the principal entity organized for sharing of information among all relevant competent authorities and for taking care that preventive or investigative action is initiated by the appropriate authorities when there is a suspicion that NPOs may be involved in TF activities as called for in c. VIII. 4.2. For investigations of TF matters, the *Länder* level Criminal Investigation Bureaus (LKA) generally takes the lead, with support from the BKA. Under Section 4 of the Act on the BKA, the BKA may also perform law enforcement tasks in order to investigate TF, especially in the case of international organized crime or when the Federal Public Prosecutor assigns the BKA to do so (in particular, in cases of special significance). For terrorist activities, investigative responsibility lies with the Federal Security Service (BfV) and the Federal Intelligence Service (BND). Each service has qualified specialists to manage such investigations. All terrorist-related suspicions receive immediate and high-level responses, including preventive against NPOs.

1129. c. VIII. 5 – The BKA is the designated point of contact to respond to international requests for information regarding police matters related to particular NPOs that are suspected of terrorism financing or other forms of terrorist support. The Federal Office for the Protection of the Constitution (BfV) is the point of contact with respect to domestic intelligence investigations. BKA and BfV reply to the requests by means of the usual communication channels.

### *Effectiveness of implementation*

1130. The German approach to preventing NPOs from being abused for TF purposes relies on transparency of the NPO sector and an intelligence-driven process to identify and respond to TF and terrorist threats. The emphasis is on the intelligence side. Germany has well established arrangements for coordinating intelligence and police efforts against terrorism, including where they involve NPOs. The groups involved have adequate capacity and are highly motivated. Where potential threats are identified, the authorities can pursue any links to NPOs and investigate possible TF activity. Law enforcement has demonstrated a willingness to take forceful measures when they are called for.

1131. The arrangements required to qualify for tax benefits – registration as an association and approval by the fiscal authorities – combined with the NPO’s own self-regulating information and control efforts provide a basic level of transparency to the tax authorities and general information to the public. The formal requirements, however, are relatively straightforward and undemanding. Satisfying the registration requirements provides limited assurance that the internal procedures called for in the Interpretative Note to SR VIII and in the 2002 International Best Practices paper are generally being followed and that NPOs will be able to respond adequately to authorities’ requests for information. STR’s related to possible TF by NPOs are uncommon. Although intelligence information on NPOs’ TF vulnerability does exist at the level of the tax authorities, generally available registration information is not sufficiently granular to allow external monitoring of NPOs for TF vulnerability either at the sectoral level or at the individual organization level. The DZI donor seal program provides an important element of transparency to the more important donors. To qualify for the DZI seal, NPOs must publish annual financial statements that provide detailed breakdowns of incomes and expenditures, as called for in 6 (b)(ii) of the Interpretative Note to SR VIII. Under the DZI seal program, participating NPOs are obliged to follow a know-your-beneficiaries and associate NPO policy, as called for in 6(b)(v). Although NPOs must demonstrate that funds are spent in a manner consistent with the objectives of the organization, there are no specific requirements that they have internal controls for this purpose, a DZI project now underway, when and if concluded, to develop a much wider database encompassing information on almost all of the NPO community would be a very useful supplement to current transparency arrangements. Renewed outreach efforts to raise awareness of TF vulnerabilities would also be useful.

#### **5.3.2. Recommendations and Comments**

1132. In order to comply fully with Special Recommendation VIII, Germany should:

- Document that NPO laws and regulations have been systematically reviewed and updated and that the vulnerability of the NPO sector is periodically reassessed.
- Require NPOs in their registration documents or in their filings for tax benefits to provide the information called for under Interpretative Note to SR VIII, Section 6 b and the financial transparency section of the 2002 FATF best practices paper.
- Energize outreach efforts to maintain awareness of TF risk in the NPO sector.

#### **5.3.3. Compliance with Special Recommendation VIII**

	Rating	Summary of factors underlying rating
SR. VIII	LC	<ul style="list-style-type: none"> <li>• Review of NPO laws and regulations and ongoing reassessments of vulnerabilities not documented.</li> <li>• Data on NPOs available from association registration documents or from tax</li> </ul>

		<p>filings for tax benefit status is sparse relative to the financial information they are expected to hold under the Interpretative Note to SR. VIII, Section 6 b, and the financial transparency section of the 2002 FATF best practices paper and is of limited usefulness for monitoring individual organizations or for sectoral monitoring.</p> <ul style="list-style-type: none"><li>• Low intensity of outreach to raise awareness of TF risk in the NPO sector, even within a strategy of safeguarding and maintaining the practice of charitable giving and the strong and diversified community of institutions through which it operates.</li></ul>
--	--	---

## 6. NATIONAL AND INTERNATIONAL COOPERATION

### 6.1. National Cooperation and Coordination (R. 31 & R. 32)

#### 6.1.1. Description and Analysis

##### *Mechanisms for Domestic Cooperation and Coordination in AML/CFT (c. 31.1):*

1133. The following mechanisms are utilized to enable policy makers, the FIU, law enforcement and supervisors, and other competent authorities to cooperate, and where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat ML and TF

1134. **The Money Laundering Contact Group** is an informal coordinating body on AML/CFT matters comprising representatives of the BMI, BMF, BMJ, and the BMWi. The latter, while a member, is not an active participant. The group was established in 1993. It meets as and when needed to coordinate AML/CFT matters across these ministries. Such needs may relate, for example, to current events, intelligence gathered by the law enforcement authorities, planned or current legislative projects, or coordination of the German position in forthcoming working group and plenary sessions of the FATF. The reason for the meetings determines the composition of the participants. Depending on the matter under discussion, supervisory authorities, law enforcement authorities, private sector representatives of reporting entities under the ML Act, the FIU and other agencies can be included in the discussions. According to the authorities, the holding of meetings of this kind guarantees a speedy, flexible, and competent discussion of important issues concerning the fight against ML and the financing of terrorism.

1135. The financial intelligence experts of the federal security authorities involved in the fight against TF hold regular meetings to exchange information and experience. The *Länder* authorities share in the exchange via the federal authorities. Information on national cooperation between the authorities involved in the work of the Joint Counter-Terrorism Centre (GTAZ) can be found in Section 2 of this report.

1136. **The FIU at the BKA** maintains contact with a range of organizations involved in the fight against ML and TF. This includes: the investigating agencies of the federal authorities and the *Länder*, the public prosecutor's offices, the customs, tax authorities (e.g. tax investigation offices), supervisory authorities, professional chambers, umbrella organizations (e.g. German Insurance Association, Central Loans Committee), entities covered under the Money Laundering Act, suppliers of special research and monitoring software, initial and further training institutions, research organizations (e.g. Max Planck Institute) and federal and *Land* ministries. Contacts are made and coordination processes discussed in the course of regular meetings, staff exchanges (e.g. job shadowing), the many lectures and training courses organized by the FIU, telephone consultations (hotline), and during the support and monitoring of specific preliminary investigations. Typical of the interaction at the FIU is its organization of annual meetings between representatives of bankers' associations, (professional) chambers, and compliance officers from major German banks, *Land* Criminal Police Offices, the Customs Criminological Office, and other special representatives of the BKA (the working group of banks and chambers, as it is called), during which there is discussion of topical issues (e.g. changes of legislation, new methods of ML and TF or the progress



made in projects such as the electronic reporting of suspicious transactions). All the participants in this discussion group feel it has proved its worth as a platform for the exchange of information and experience.

1137. The Joint Financial Investigation Groups (GFGs) at the *Länder* Criminal Police Offices discharge their duties in such a way as to ensure continuous coordination of specialist and operational matters relating to criminal prosecution. Police and customs authorities work together in these GFGs as equal partners on criminal investigations into ML offenses, in which the BKA and its FIU may be involved as required.

1138. A link between the BaFin and the FIU exists in the area of STRs, which are reported directly to the FIU. The information exchange between the authorities is unproblematic and provided for by Section 9 (1) number 1 of the ML Act. However, there are no significant areas in which the jurisdiction of the BaFin and FIU overlap, which is why institutionalized cooperation has not been deemed necessary so far. However, the assessors could not establish that the FIU passed on information about the quality of STR reporting to help inform the BaFin's supervision of reporting entities.

1139. The BaFin cooperates directly with the *Länder* police's relevant investigative units when taking its own enforcement actions. In the BaFin's MLPG, this is done only by section GW 3, which prosecutes illegal money remittance, foreign currency exchange, and credit card businesses.

1140. There is also considerable informal knowledge exchange between the BaFin and the FIU on, inter alia, FATF typology papers, EU twinning projects (most recently Albania), the BaFin providing training for BKA financial investigations workshops, the BKA providing lectures for the BaFin's "Praxisforum," coordination regarding the freezing of assets under Section 6a of the Banking Act, as well as the transmission of copies of particular STRs and other information through the FIU. In addition, a member of the FIU spent some time working with the MLPG in order to further improve understanding and coordination between the authorities.

### ***Effectiveness of policies and programs***

1141. The authorities indicated that there have been regular assessments of the existing system relating to the prevention of ML and TF carried out by the authorities involved in prevention. They gave the following examples:

- The FIU publishes an annual report providing an overview of the suspicious operations notified as well as an indication of the financial entities, nonfinancial businesses and professions that are most active on this issue. Part of the report is dedicated to the implementation of the Third EU Money Laundering Directive.
- The BaFin publishes an annual report, which gives an overview of its activities and important events and developments during the reporting period. This also includes a chapter on the activities of the BaFin's AML Group and the essential findings resulting from its AML-supervisory tasks. The BaFin also regularly holds meetings with Associations of the Financial Sector in Germany (*e.g.* Federal Association of German Banks or the German Insurance Association), in which practical issues pertaining to the implementation and interpretation of the AML/CFT requirements are discussed. In this context, the effectiveness of practical procedures and supervisory requirements is also discussed.
- In order to ensure the proper implementation of the German AML/CFT provisions, there are periodical meetings between the authorities and financial and nonfinancial bodies (*Verbände und Kammervertretungen*) to discuss the potential difficulties in applying existing legal provisions.

These meetings have led to improvements in procedures, such as the feedback for entities which notify the authorities of suspicious or unusual operations.

- There are also regular meetings of the German delegation to the FATF which, in its regular form, includes representatives from the Federal Ministry of Finance, the supervisory authorities for the financial system (the BaFin and *Bundesbank*), the Federal Ministry of Economics and Technology, the Federal Ministry of the Interior, and the FIU where there is discussion of the system as it stands, work on projects aimed at improving procedures and work on projects for modifying legislation, with suggestions passed on to the Government. The delegation has also been heard on proposals to amend legislation on the subject of ML.
- Once a year, the German Government surveys the federal authorities about the implementation of government measures relevant to combating terrorism. This survey also covers measures and projects to combat TF.

***Additional Element – Mechanisms for Consultation Between Competent Authorities and Regulated Institutions (c. 31.2):***

1142. As mentioned above, from time to time, representatives of the private sector are invited to participate in discussions with the authorities. However, this is ad hoc, and there is no formal mechanism that provides for regular consultation between the authorities and the institutions.

***Analysis of Effectiveness***

1143. The authorities have a variety of mechanisms in place to facilitate cooperation and policy development, albeit informal and ad hoc. There are also effective mechanisms to facilitate cooperation between the agencies involved in investigating ML and TF. One area where there seemed to be a lack of engagement was from the authorities responsible for many of the DNFBPs.

1144. The prime motivation for implementing Germany's AML/CFT regime appeared to be aimed at implementing the Third EU Directive and to being compliant with the FATF 40+9 Recommendations. However, the assessors were not provided with any minutes of meetings or evidence of processes to follow up on issues raised during national coordination efforts. Moreover, the MoF appeared under-resourced to coordinate national implementation as well as Germany's position within the FATF.

1145. The assessors also gained the impression that there was more focus on coordinating policy positions at the FATF on international matters than on coordinating domestic implementation of Germany's AML/CFT regime.

1146. There was also no hard evidence of any national level efforts aimed at reviewing the effective implementation of the regime – and it was clear that one possible reason for this was that the authorities do not appear to have any direct accountability to report on AML/CFT matters within the German political system (*i.e.* no reporting to the parliament). Moreover, none of the main policy ministries report on AML/CFT matters in their annual reports. The practical implementation is best illustrated by reference to the fact that, despite a belief on the part of the national policy ministries that a main focus for Germany's AML/CFT regime was to fight tax evasion, the assessors could not find much effective implementation of the regime that that was consistent with that belief.

***6.1.2. Recommendations and Comments***

1147. In order to comply fully with Recommendations 31 and 32 (cr. 32.1), Germany should:

- Ensure that the ML Contact Group meetings include a focus on national implementation of Germany's AML/CFT regime.
- Put in place formal mechanisms to review the effectiveness of Germany's AML/CFT system.
- Fully engage authorities responsible for DNFBPs.
- Have the FIU provide the BaFin with information about the quality of STRs received from reporting entities.
- Put in place formal mechanisms to enhance dialogue with the private sector.
- Provide more resources to the MoF for it to coordinate national implementation.

### 6.1.3. *Compliance with Recommendation 31 & 32 (criterion 32.1 only)*

	Rating	Summary of factors underlying rating
<b>R.31</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• No effective coordination with authorities responsible for DNFBPs.</li> <li>• Policy coordination focuses primarily on FATF policy matters rather than developing policies and activities to combat ML and TF in Germany.</li> </ul>
<b>R. 32</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• No evidence that overall reviews of effectiveness of the German AML/CFT system have been undertaken.</li> </ul> <p>Rating for this section: <b>NC</b></p>

## 6.2. **The Conventions and UN Special Resolutions (R.35 & SR.I)**

### 6.2.1. *Description and Analysis*

#### ***Ratification of AML Related UN Conventions (c. 35.1):***

1148. Germany signed the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention) on January 19, 1989 and ratified it on July 22, 1993. The convention was passed into law by virtue of the Act of August 2, 1993 to Implement the United Nations Convention of December 20, 1988 Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Implementing Act Narcotic Drugs Convention 1988), which entered into force on February 28, 1994.

1149. Germany signed the 2000 United Nations Convention Against Transnational Organized Crime (the Palermo Convention) on December 12, 2000 and ratified it on June 14, 2006. The convention entered into force on July 14, 2006.

#### ***Ratification of CFT Related UN Conventions (c. I.1):***

1150. Germany signed the 1999 International Convention for the Suppression of the Financing of Terrorism (the CFT) on July 20, 2000 and ratified it on June 17, 2004). The convention entered into force on July 17, 2004.

***Implementation of Vienna Convention (Articles 3-11, 15, 17 & 19, c. 35.1):***

1151. As described in Section 2.1 of this report, Germany has enacted legislation that implements the key AML requirements of the Vienna Convention. Proper ancillary offenses as well as the association to commit ML are criminalized by the law. Germany has also criminalized the trafficking in narcotics and other related offenses.

1152. The criminal law and the criminal procedures laws provide for provisional measures and for forfeitures and confiscations of property. Controlled deliveries are also available for use by investigators.

***Implementation of CFT Convention (Articles 2-18, c. 35.1 & c. I.1):***

1153. As described under Special Recommendation II, Germany has enacted legislation that is partially consistent with the CFT convention; The definition of “serious violent act endangering the state” is not fully consistent with the CFT Convention as it does not extend to all acts that constitute offenses within the scope of, and as defined in the treaties annexed to the CFT Convention. A serious violent act endangering the state is narrower in scope than the generic definition of terrorist act under Article 2 of the CFT Convention as it does not cover serious bodily injuries. The definition of the term “funds” in connection with the financing of a terrorist act or individual terrorist is not fully in line with the requirements of the CFT Convention, as it imposes a requirement for the funds to be of a certain minimum value (*i.e.* not merely insubstantial). Germany has acceded to all of the nine treaties, conventions, and protocols listed in the CFT Convention’s Annex.

***Implementation of Palermo Convention (Articles 5-7, 10-16, 18-20, 24-27, 29-31 & 34, c. 35.1):***

1154. Previous sections of this report show that Germany has enacted legislation to implement some of the key AML requirements of the Palermo Convention. However, significant gaps still remain, such as the inability to apply the ML offense to persons that commit and are convicted for the predicate offense, or the fact that “insider trading and market manipulation” and “counterfeiting and piracy of products” are not predicate offenses to ML. Moreover, a number of categories of predicate offenses for ML contain offenses that are only considered predicate offenses if certain aggravating circumstances are also met. Natural and legal persons are not subject to sanctions that take into account the gravity of the ML offense.

1155. The CC punishes offenses dealing with criminal organizations as well as appropriate ancillary offenses. Criminal liability does not extend to legal persons due to fundamental principles of German law. The criminal law and the criminal procedures laws provide for provisional measures and for forfeitures and confiscations of property.

1156. Prosecution authorities have a range of special techniques of investigation at their disposal pursuant to the CPC and the guidelines for conducting criminal investigations, including telephone taps, undercover agents, controlled delivery and informants.

1157. In the area of international cooperation, Germany has enacted legislation that enables it to provide a wide range of mutual legal assistance. Germany does not extradite its nationals but, when faced with such cases, it automatically proceeds to submit the case without undue delays to its competent authorities for the purpose of prosecution.

***Implementation of UNSCRs relating to Prevention and Suppression of TF (c. I.2)***

1158. Mechanisms have been put in place for the implementation of United Nations Security Council Resolutions (UNSCRs) 1267 and 1373. The UNSCRs relating to the prevention and suppression of the financing of terrorism are implemented in Germany within the EU-framework by means of community

legislation. UNSCRs 1267 (1999) and 1390 (2002) as well as 1455 (2003) are implemented by Council Regulation No. 881/2002 of May 27, 2002, whereas the relevant parts of UNSCR 1373 (2001) are implemented by Council Regulation 2580/2001 of December 27, 2001. The Council regulations are directly applicable law in Germany. However, the following shortcomings still remain in this area: *i)* except for credit institutions, financial services institutions and investment companies, no other person is subject to directly applicable requirements for the freezing of assets for EU-internals under S/RES/1373; *ii)* there is a lack of effective procedures making it possible to freeze assets other than funds in many instances (*i.e.* for EU-internals where the Banking Act applies); and *iii)* there are no appropriate measures to monitor effectively the compliance with obligations under SR.III by persons and entities other than financial institutions and “companies.”

***Additional Element – Ratification or Implementation of Other relevant international conventions (c. 35.2):***

1159. Germany signed the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism on November 8, 1990 and ratified it on September 16, 1998. The convention entered into force on January 1, 1999. The convention sets out the provisions needed to ensure compliance with requests for the execution of foreign orders on confiscation or forfeiture or to enable such requests to be submitted.

**6.2.2. Recommendations and Comments**

1160. In order to implement fully Recommendation 35 and Special Recommendation I, Germany should:

***With respect to Recommendation 35:***

- Fully implement the Palermo Convention by criminalizing self-laundering.
- Fully implement the Palermo Convention by making “insider trading and market manipulation” and “counterfeiting and piracy of products” predicate offenses for ML, amending the CC to ensure that predicate offenses for ML include a range of offenses in each of the designated categories of offenses without having to meet the additional requirement that the offense is committed with the intention to make a profit or by a member of a gang founded for the recurrent commission of such an offense, and increasing the minimum and maximum ranges consistent with the level of penalties for other serious offenses in Germany.

***With respect to Special Recommendation I:***

- Fully implement the CFT Convention by amending Section 89a of the CC to extend the financing of a terrorist act and of an individual terrorist to all acts that constitute offenses within the scope of, and as defined in the treaties annexed to the CFT Convention, to cover serious bodily injuries, and to eliminate the requirement for the “funds” to be of a certain minimum value (*i.e.* not merely insubstantial).
- Enact legislation to make S/RES/1373 applicable to any entity or persons other than credit institutions, financial services institutions, and investment companies for the freezing of assets concerning EU-internals.

- Set up procedures within Germany that will ensure in all cases the freezing without delay of assets other than funds (such as immovable goods, companies and businesses and vehicles) for cases of EU-internals where the Banking Act applies.
- Set up appropriate measures to monitor effectively the compliance with freezing obligations by persons and entities other than financial institutions and “companies.”

### 6.2.3. Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R. 35	PC	<p>Germany has not fully implemented the Palermo Convention:</p> <ul style="list-style-type: none"> <li>• The ML offense cannot be applied to persons who commit and are convicted for the predicate offense. The inability to do this is not supported by principles that amount to fundamental principles under the FATF standards.</li> <li>• “Insider trading and market manipulation” and “counterfeiting and piracy of products” are not predicate offenses to ML.</li> <li>• Natural and legal persons are not subject to effective, proportionate, and dissuasive sanctions for basic ML.</li> </ul>
SR. I	PC	<p>Germany has not fully implemented the Terrorism Financing Convention and the relevant UNSCR:</p> <ul style="list-style-type: none"> <li>• The definition of “serious violent act endangering the state” is not fully consistent with the CFT Convention as it does not extend to all acts that constitute offenses within the scope of, and as defined in the treaties annexed to the CFT Convention and it does not cover serious bodily injuries.</li> <li>• The definition of the term “funds” in connection with the financing of a terrorist act or individual terrorist is not fully in line with the requirements of the CFT Convention, as it imposes a requirement for the funds to be of a certain minimum value (<i>i.e.</i> not merely insubstantial).</li> <li>• The financing to carry out a terrorist act and the financing of an individual terrorist are not fully consistent with the CFT Convention.</li> <li>• Except for credit institutions, financial services institutions, and investment companies, no other person is subject to directly applicable requirements for the freezing of assets for EU-internals under S/RES/1373.</li> <li>• Effectiveness not established: lack of specific statistics to establish that natural and legal persons are subject to effective, proportionate, and dissuasive sanctions and that the TF offenses are being effectively implemented.</li> <li>• Lack of effective procedures making it possible to freeze assets other than funds for EU-internals where the Banking Act applies.</li> <li>• There are no appropriate measures to monitor effectively the compliance with freezing obligations by persons and entities other than financial institutions and “companies.”</li> </ul>

## 6.3. Mutual Legal Assistance (R.36-38, SR.V)

### 6.3.1. Description and Analysis

#### Legal Framework

1161. The type and extent of international cooperation that Germany may provide is mainly regulated by the Law on International Assistance in Criminal Matters of December 23, 1982 (LIACM), the Guidelines on Relations with Foreign Countries in Criminal Law Matters (the Guidelines), which were



revised with effect from January 1, 2009, the international conventions to which Germany is a party, and by other multilateral and bilateral agreements concluded. Where an international treaty exists, the LIACM will only be applied to cases which are not, or not conclusively, covered by the treaty concerned.

1162. In accordance with Article 32 of the Basic Law, legal assistance in criminal matters, which comes under the maintenance of relations with foreign countries, is the responsibility of the federal government.

***Widest Possible Range of Mutual Assistance (c. 36.1)***

1163. Germany is capable of providing comprehensive, effective, and timely judicial assistance. However, the deficiencies in the ML offense, noted under Recommendation 1, may impact on the ability of Germany to provide certain forms of international cooperation where dual criminality is required (*i.e.* extraditions), particularly for non-EU jurisdictions. Such impact may likely be limited given the exceptional circumstances where dual criminality is required, and the lack of unduly restrictive requirements. Despite the lack of statistics, the authorities have assured assessors that no requests for MLA have ever been denied by Germany, or rejected by other countries upon a request by Germany, on the basis of dual criminality requirements not being met because of the deficiencies in the ML offense.

1164. The LIACM is the basis for mutual legal assistance in the absence of a treaty. Requests submitted by countries may be granted pursuant to Section 59 of the LIACM in combination with the relevant provisions of the CPCF. Section 59 provides that “*At the request of a competent authority of a foreign state, other legal assistance in criminal matters may be provided. Such legal assistance shall be any type of aid given to foreign criminal proceedings regardless of whether the foreign proceedings are conducted by a court or by a governmental authority and whether the legal assistance is to be provided by a court or a governmental authority. Legal assistance may be provided only under circumstances under which German courts and governmental authorities could render legal assistance to each other.*” The provision refers broadly to “any type of aid” and can, therefore, be considered to comprise all of the separate natures of mutual legal assistance referred to by criterion 36.1.

1165. The surrender of objects (the Act uses the term “objects” – *Gegenstände* – which, as mentioned under Recommendation 1, is not defined under German law) and documents to provide evidence in a foreign criminal proceeding is governed by Section 66 (1) of the LIACM. The provision sets forth that at the request of a competent authority of a foreign state, property may be surrendered which may serve as evidence in foreign proceedings (66 (1) Number 1), or which the person involved or a participant has obtained for or from the offense forming the basis for the request (Number 2), or which the person involved or participant has obtained or has taken as benefit as a result of the sale of an object obtained or as compensation for its destruction, damage, withdrawal or on the basis of an acquired right (Number 3), or which emanated from the offense on which the request is based or was used or intended for use in its commission or preparation (Number 4).

1166. The authorities explained that Section 66 should be interpreted broadly as authorizing the surrender of all property and rights. Other qualifying conditions follow from Section 66(2) of the LIACM, such as the existence of dual criminality, the existence of a seizure order from the requesting state and other assurances (*i.e.* that the right of third parties will not be impaired, with the reservation that objects surrendered will be returned immediately upon request). This provision is intended for the surrender of property which may serve as evidence or which the person involved or a participant has obtained as a result of the offense forming the basis for the request, or which he obtained in exchange for such objects, or which emanated from the offense on which the request is based or was used or intended for use in its commission or preparation (Section 66 (1) LIACM). It can, therefore, be used for the confiscation of assets

laundered or intended to be laundered, the proceeds of ML and assets used or intended to be used for TF, or the instrumentalities of such offenses and assets of corresponding value (§§ 67 (1), 66 (1)).

1167. Pursuant to Section 67(1) of the LIACM, property under consideration for surrender to a foreign country can be seized or otherwise impounded prior to receipt of a request for its surrender. Section 67(1) further adds that a search may also be conducted for this purpose. Pursuant to Section 67(2), property may also be seized or otherwise impounded under certain conditions if this is necessary to comply with a request that does not seek to secure surrender of the property (for example, a foreign country requests information from written documents in the possession of private individuals who are not willing to surrender them temporarily to the authority conducting the examination).

1168. Where bilateral or multilateral treaties have been concluded between Germany and other states, mutual assistance relations are primarily governed by these treaties. Germany has signed the following MLA treaties:

**Statistical Table 28: Treaties of the Council of Europe**

Treaty		Entry into Force for Germany
European Convention on Extradition	CETS No.: 024	01.01.1977
Second Additional Protocol to the European Convention on Extradition	CETS No.: 098	05.06.1983

Additional Bilateral Treaties between the Federal Republic of Germany and:

Treaty		Entry into Force for Germany
The Republic of Italy	BGBI. 1982 II, 106; 1985 II, 835	04.07.1985
The Kingdom of the Netherlands	BGBI. 1981 II, 1153; 1983 II, 32	30.01.1983
The Republic of Austria	BGBI. 1975 II, 1163; 1976 II, 1798	01.02.1977
The Swiss Confederation	BGBI. 1975 II, 1176; 1976 II, 1798	01.01.1976
- Amending Treaty	BGBI. 2001 II, 946; 2002 II, 606	01.03.2002
The Czech Republic	BGBI. 2001 II, 726; 2002 II, 1043	19.06.2002
The Republic of Poland	BGBI. 2004 II, 522, 1339	04.09.2004

Treaty		Entry into Force for Germany
European Convention on Mutual Assistance in Criminal Matters	CETS No.: 030	01.01.1977
Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters	CETS No.: 099	12.04.1982

## Additional Bilateral Treaties between the Federal Republic of Germany and:

Treaty		Entry into Force for Germany
The French Republic	BGBI. 1978 II, 329; 1980 II, 1435	01.01.1981
The State of Israel	BGBI. 1980 II, 1334; 1981 II, 94	06.03.1981
The Republic of Italy	BGBI. 1982 II, 111; 1985 II, 836	04.07.1985
The Kingdom of the Netherlands	BGBI. 1981 II, 1158; 1983 II, 32	30.01.1983
The Kingdom of the Netherlands on Cross-Border Cooperation in Police Matters and in Criminal Matters	BGBI. 2006 II, 194	23.03.2006
The Republic of Austria	BGBI. 1975 II, 1157; 1976 II, 1818	01.02.1977
The Republic of Austria on Cross-Border Cooperation in Police Matters and in Criminal Matters	BGBI. 2005 II, 858, 1307	01.12.2005
The Swiss Confederation	BGBI. 1975 II, 1171; 1976 II, 1818	01.01.1977
- Amending Treaty	BGBI. 2001 II, 946; 2002 II, 607	01.03.2002
The Swiss Confederation on Cross-Border Police and Judicial Cooperation	BGBI. 2001 II, 946; 2002 II, 608	01.03.2002
The Czech Republic	BGBI. 2001 II, 765; 2002 II, 1163	19.06.2002
The Republic of Poland	BGBI. 2004 II, 537, 1339	04.09.2004

Treaty		Entry into Force for Germany
European Convention on Information on Foreign Law	CETS No.: 062	19.03.1975
Additional Protocol to the European Convention on Information on Foreign Law	CETS No.: 097	24.10.1987
European Convention on the Suppression of Terrorism	CETS No.: 090	04.08.1978
Convention on the Transfer of Sentenced Persons	CETS No.: 112	01.01.1985
Additional Protocol to the Convention on the Transfer of Sentenced Persons	CETS No.: 167	01.08.2007
European Convention on the Compensation of Victims of Violent Crimes	CETS No.: 116	01.02.1988
Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime	CETS No.: 141	25.05.1995
Agreement on illicit traffic by sea, implementing Article 17 of the United Nations	CETS No.: 156	01.05.2000

	Convention against illicit traffic in narcotic drugs and psychotropic substances		
	Convention on Cybercrime	CETS No.: 185	01.07.2009

**Statistical Table 29: Multilateral Treaties of the European Union**

Treaty		Entry into Force for Germany
Council Framework Decision on the European arrest warrant and the surrender procedures between Member States of the European Union	2002/584/JHA	02.08.2006
Convention on extradition between Member States of the European Union	Official Journal C 313 of 23.6.1996; BGBl. 1998 II, 2253	11.08.1998
Convention on simplified extradition procedure between the Member States of the European Union	Official Journal C 78 of 30.03.1995; BGBl. 1998 II, 2229	12.09.1998
Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union	Official Journal C 197 of 12.07.2005; BGBl. 2005 II, 650	02.02.2006
Protocol to the Convention on Mutual Assistance in Criminal Matters	Official Journal C 326 of 21.11.2001; BGBl. 2005 II, 661	02.02.2006
Council Framework Decision on the execution in the European Union of orders freezing property or evidence	2003/577/JI	02.08.2003
Convention between the Member States of the European Communities on the enforcement of foreign criminal sentences		15.07.1997
Council Framework Decision on the Application of the Principle of Mutual Recognition to Financial Penalties	2005/214/JHA	22.04.2005
Council Framework Decision on the application of the principle of mutual recognition to confiscation orders	2006/783/JHA	24.11.2006
Council Framework Decision on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters	2008/978/JHA	19.01.2009
Convention Implementing the Schengen Agreement	BGBl. 1996 II, 242	26.03.1995

**Statistical Table 30: Multilateral Treaties of the United Nations**

Treaty		Entry into Force for Germany
Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances	453 UNTS 85; BGBl. 1993 II, 1137; 1994 II, 496	28.02.1994
Convention against Transnational Organized Crime	BGBl. 2005 II, 956; 2007 II, 1311	14.06.2006
Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children	BGBl. 2005, 956; 2007 II, 1341	14.07.2006

	Protocol against the Smuggling of Migrants by Land, Air and Sea	BGBI. 2005, 956	
--	---	-----------------	--

**Statistical Table 31: Bilateral Extradition Treaties between the Federal Republic of Germany and**

	Treaty		Entry into Force for Germany
	Australia	BGBI. 1990 II, 111, 716	01.08.1990
	Canada	BGBI. 1979 II, 665, 1049	30.09.1979
	- Additional Treaty	BGBI. 2004 II, 973, 1564	23.10.2004
	The United States of America	BGBI. 1980 II, 646, 1300	29.08.1980
	- Additional Treaty	BGBI. 1988 II, 1087; 1993 II, 846	11.03.1993
	The Republic of India	BGBI. 2003 II, 1634; 2004 II, 787	28.05.2004



**Statistical Table 32: Bilateral Mutual Legal Assistance Treaties between the Federal Republic of Germany and**

Treaty		Entry into Force for Germany
The Swiss Confederation	See Bilateral Additional Treaties on European Convention on Mutual Assistance in Criminal Matters, above	
United States of America (Agreement on legal assistance in penal matters and penal register information; Combating Illicit Trafficking in Narcotic Drugs)	BGBI. 1961 II 471; BGBI. 1957 II 709	03.01.1961 24.08.1955
Canada	BGBI. 2004 II 963, 1564	23.10.2004
Thailand	BGBI. 1995 II 1011; 1996 II, 1220	19.06.1996

1169. Separate mutual assistance provisions are also contained in offense-related conventions such as the United Nations Convention of December 20, 1988 against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.

1170. Mutual legal assistance between Germany and other EU members is regulated by the Council Framework Decision of July 22, 2003 on the execution in the European Union of orders freezing property or evidence (Framework Decision on Freezing) which covers (without exception) the freezing of property or evidence. Adjustments to German law in order to implement the Framework decision on Freezing were made in the Law Implementing the Framework Decision on Freezing, which came into force on June 30, 2008.

1171. The Framework Decision on Freezing entails an obligation to waive verification of dual criminality in the event of the surrender of property as evidence in connection with one of the total of 32 offense categories listed in the Framework Decision – this includes ML and acts of terrorism, so to that extent, the problems related to deficiencies in the ML offense might not apply. It also reduces the type and number of justifications for rejecting the legal assistance requested, and provides for a speeding up of the freezing procedures. The requested country is expected to decide on recognition of the requesting country's seizure decision as quickly as possible, if possible within 24 hours of receiving the request. Furthermore, following recognition of the seizure decision, the responsible judicial authorities in the requested country must immediately take the requisite steps to ensure prompt implementation just as they would do if a decision on seizure had been announced by an authority of the requested country. The Framework Decision on Freezing is supplemented by Council Framework Decision 2006/783/JHA of October 6, 2006 on the application of the principle of mutual recognition to confiscation orders (Framework Decision on Confiscation), which also applies to ML and acts of terrorism. The Framework Decision on Confiscation has been implemented through a legislative act adopted on September 19, 2009 and which entered into force on October 22, 2009.

***Provision of Assistance in Timely, Constructive and Effective Manner (c. 36.1.1)***

1172. Germany is capable of granting rapid and effective legal assistance. Pursuant to Number 19(1) of the Guidelines, decisions on the granting of requests for legal assistance must be brought for authorization without delay. While the Guidelines do not state that the actual decision on authorization or refusal must be issued without delay, the authorities stated that authorizations are granted in a rapid manner.

1173. In addition, pursuant to number 22(1) of the Guidelines, the enforcing authorities must always execute the requests in accordance with the same provisions as would apply if the request had been submitted by a German authority.

1174. Pursuant to number 22(2) of the Guidelines, mutual assistance shall in principle not be executed prior to the ruling of the authorizing authority. The executing authority may exceptionally execute the mutual assistance where a delay is likely to jeopardize the success of the investigation if there are no objections to rendering mutual assistance. If the mutual assistance has been previously executed, the executing authority shall forward the request and the documents in proof of execution to the authorizing authority.

1175. Pursuant to Article 2 (2) second sentence of the German Basic Law (*Grundgesetz*, GG), requests for legal assistance in cases involving detention will always be classified as urgent. In addition, the urgency of a request may result from the content of the investigation sought, e.g. in cases of attachment or where there is a need for swift preservation of evidence through search and seizure.

1176. There are also special acceleration requirements for judicial assistance among Member States of the European Union, such as in Article 5(3) of the Framework Decision on Freezing (see 36.1).

1177. However, in the absence of statistics on mutual legal assistance, assessors were unable to evaluate the effectiveness of the system.

#### ***No Unreasonable or Unduly Restrictive Conditions on Mutual Assistance (c. 36.2)***

1178. Pursuant to Section 73 of the LIACM, legal assistance is not granted by German authorities if it would contravene essential principles of the German legal system (*ordre public proviso*). In accordance with the decisions of the Federal Constitutional Court on the *ordre public* principle, legal assistance must be rejected if the acts on which the request for assistance are based no longer conform with minimum standards of elementary constitutional justice under international law, the inalienable constitutional principles of public order in Germany, or elementary requirements under international law. Particular importance is attached in this regard to ensuring respect for the principle of the rule of law, including the principle of proportionality, as well as the preservation of human dignity. Section 73 of the LIACM applies especially in cases of extradition but may also apply in other forms of international cooperation, such as the cross-border execution of prison sentences and imposition of fines, forfeitures and confiscations, or the surrendering of property to another country. While no statistics were provided, the authorities have confirmed that a very small number of requests have been rejected by application of this provision.

1179. Dual criminality is a strict requirement under German law only in the area of extraditions (see Section 3 of the LIACM). In the areas of “enforcement assistance” (*i.e.* in the cross-border execution of prison sentences and imposition of fines, forfeitures and confiscations) and “other legal assistance” (*i.e.* support for other countries in investigation proceedings), German law does not generally require dual criminality. In principle, the existence of criminal or administrative fine proceedings in the requesting country is sufficient. The requirement of dual criminality in the area of “other legal assistance” is only expressly required for the seizure and surrender of property (Sections 66 and 67 of the LIACM) and for requests that are targeted at investigation measures under criminal law, and that under national law require an offense to have been committed (Section 59 (3) in conjunction with Section 77 of the LIACM). This concerns in particular sensitive investigation measures such as the surveillance of telecommunications or the acoustic surveillance of a private residence (Sections 100a, 100c of the CPC).

1180. In the field in which the legal instruments of the European Union are applied to the mutual recognition of judicial decisions (such as the Framework Decision on the execution in the European Union

of orders freezing property or evidence), the requirement for dual criminality is dispensed with for most major offenses, including ML and TF.

1181. In cases in which the granting of legal assistance is contingent upon dual criminality, German legislation does not require full agreement in the definitions of criminal offenses, including any subjective elements of an offense. It is sufficient for the act to meet the requirements of national law after analogous conversion of the facts (cf. Section 3(1) of the LIACM). A different legal classification is not prejudicial either, as long as the facts of the case concerned infringe some criminal provision of the requested state, the purpose of which can also be to safeguard a completely different legal interest.

### ***Efficiency of Processes (c. 36.3)***

1182. The processes in place for the execution of mutual legal assistance appear to be clear.

1183. In accordance with Article 32 of the Basic Law, legal assistance in criminal matters, which comes under the maintenance of relations with foreign countries, is the responsibility of the federal government. In accordance with Section 74(1) of the LIACM, therefore, the authority granting approval is always the Federal Ministry of Justice, which makes its decisions in agreement with the Federal Foreign Office and other federal ministries whose portfolio is affected by the request for legal assistance. If responsibility for the provision of legal assistance rests with an authority belonging to the portfolio of a different federal ministry, the decision would then rest with such ministry rather than the Federal Ministry of Justice.

1184. Pursuant to Section 74(1) third sentence of the LIACM, the Federal Ministry of Justice has transferred its competence deriving from Section 74(1) of the LIACM to the Federal Office of Justice (situated in Bonn), which belongs to the portfolio of the Federal Ministry of Justice.

1185. Furthermore, pursuant to Section 74(2) of the LIACM, the federal government has largely transferred its right to decide on foreign requests for legal assistance and to request legal assistance from other countries to the *Länder* by way of an agreement on jurisdiction with the *Länder* (revised version of April 28, 2004, Federal Gazette p. 11 494). By virtue of this agreement, the enforcement authority for legal assistance requests is always the locally responsible public prosecutor with the Regional Court. This reflects the principle of direct transmission of foreign orders and requests required by many European Union legal instruments.

1186. The Guidelines also comprise a list of issuing and receiving authorities, border towns and penal institutions. In addition, they contain a large number of forms and samples designed to facilitate application of the guidelines. These Guidelines thus offer all the bodies concerned with legal assistance on criminal matters practical recommendations which help to standardize and facilitate the entire process of judicial assistance.

1187. While the processes for the execution of mutual legal assistance requests appear to be clear, in the absence of statistics, assessors were unable to evaluate the efficiency of the process.

### ***Provision of Assistance Regardless of Possible Involvement of Fiscal Matters (c. 36.4)***

1188. According to the authorities, national legislation does not provide for any refusal of requests for mutual legal assistance on the sole grounds that fiscal matters are affected. In this respect Germany has undertaken commitments in various international conventions; cf. for example, Article 1 of the (First) Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ZP-EuRgÜbk)

and Article 18(22) of the United Nations Convention of November 15, 2000 against Transnational Organized Crime (UNTOC).

***Provision of Assistance Regardless of Existence of Secrecy and Confidentiality Laws (c. 36.5)***

1189. The authorities have also assured that under German law, “secrecy” does not stand in the way of measures in the field of international legal assistance. Accordingly, a request for mutual legal assistance would, therefore, not be refused on the grounds of laws that impose secrecy or confidentiality requirements on financial institutions. However, the restrictions faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by professional privileges (*i.e.* lawyers and notaries) limit Germany’s ability to deliver mutual legal assistance where such DNFBPs are involved.

***Availability of Powers of Competent Authorities (applying R.28, c. 36.6)***

1190. The powers of competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance. In accordance with Number 22 (1) first sentence of the Guidelines, requests for legal assistance must always be executed in accordance with the same provisions that would apply if the request had been made by a German authority. See Section 36.3.

***Avoiding Conflicts of Jurisdiction (c. 36.7)***

1191. Germany has considered introducing mechanisms to transfer prosecution to other states and has come to the conclusion that no greater need for action is seen in this field to institute any specific mechanisms. The reason is that, according to experience gained thus far in Germany, the transfer of criminal proceedings does not pose any practical problems. However, at the European level, the competent work groups of the European Council are deliberating the suggestion to take a Framework Decision on the issue of “Transfer of Proceedings in Criminal Matters.” The suggestion is targeted at making procedural rules available according to which the judicial authorities of a member state of the European Union might transfer an ongoing preliminary criminal investigation or ongoing criminal proceedings to the judicial authorities of another member state. These should then be obligated in principle to accept the criminal proceedings unless specific reasons for refusing to do so govern. In the event of prosecution being accepted, the proceedings in the state transferring them shall be suspended or discontinued. The negotiations on the Framework Decision are at a relatively early stage and it is not to be expected that the Framework Decision will be taken by the Council during 2009.

***Additional Element – Availability of Powers of Competent Authorities Required under R28 (c. 36.8)***

1192. Whether direct channels of communication are opened depends on the relevant applicable treaty-based provisions. Pursuant to Number 5(2) of the Guidelines, diplomatic channels must always be used in cases of non-treaty-based mutual legal assistance. In accordance with Number 17(1) of the Guidelines, if a request is submitted through an unauthorized channel, it must nevertheless be approved, provided that there are no other impediments. Number 17(2) further provides that if a request has not been submitted to a responsible authority, it must immediately be forwarded to the responsible authority.

1193. The powers described under Recommendation 28 are also available for use in response to requests for mutual legal assistance. See Section 36.6.

***International Cooperation under SR V (applying c. 36.1-36.6 in R. 36, c. V.1) and Additional Element under SR V (applying c. 36.7 & 36.8 in R.36, c. V.6)***

1194. The provisions described above apply equally to the fight against terrorism and TF. It should be noted, however, that the deficiencies described under Special Recommendation II impact on Germany's ability to provide mutual legal assistance in cases where dual criminality is a precondition (*i.e.* extradition, enforcement assistance, forfeitures, confiscations, and certain types of "other assistance," such as seizures or freezes where property is to be surrendered), especially in non-EU jurisdictions.

***Dual Criminality and Mutual Assistance (c. 37.1 & 37.2)***

1195. Dual criminality is only strictly required for extradition. In the areas of "enforcement assistance" (*i.e.* in the cross-border execution of prison sentences and imposition of fines, forfeitures and confiscations) and "other legal assistance" (*i.e.* support for other countries in investigation proceedings), German law does not generally require dual criminality. In principle, the existence of criminal or administrative fine proceedings in the requesting country is sufficient. The requirement of dual criminality in the area of "other legal assistance" is only expressly required for the seizure and surrender of property (Sections 66 and 67 of the LIACM) and for requests that are targeted at investigation measures under criminal law, and that under national law require an offense to have been committed (Section 59 (3) in conjunction with Section 77 of the LIACM). This concerns in particular sensitive investigation measures such as the surveillance of telecommunications or the acoustic surveillance of a private residence (Sections 100a, 100c of the CPC). Apart from these exceptions, the provision of "other forms" of mutual legal assistance, in particular for less intrusive and noncompulsory measures in support of foreign criminal proceedings, may be rendered in the absence of dual criminality.

1196. In cases such as extradition, in which the granting of legal assistance is contingent upon dual criminality, German legislation does not require full agreement in the definitions of criminal offenses, including any subjective elements of an offense. It is sufficient for the act to meet the requirements of national law after analogous conversion of the facts (*cf.* Section 3(1) of the LIACM). A different legal classification does not pose an impediment either, as long as the facts of the case concerned infringe a criminal provision of the requesting state, the purpose of which can also be to safeguard a completely different legal interest.

1197. It should be noted, however, that the deficiencies in the ML offense described under Recommendation I may impact on Germany's ability to provide mutual legal assistance where dual criminality is a precondition, especially for non-EU jurisdictions. Such impact may likely be limited given the exceptional circumstances where dual criminality is required and the lack of unduly restrictive requirements. Despite the lack of statistics, the authorities have assured assessors that no requests for MLA have ever been denied by Germany, or rejected by other countries upon a request by Germany, on the basis of dual criminality requirements not being met because of the deficiencies in the ML offense. The authorities do not share the assessors' concerns about this point.

1198. Finally, the limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by professional privileges (*i.e.* lawyers and notaries) may limit Germany's ability to deliver mutual legal assistance where such DNFBPs are involved.

***International Cooperation under SR V (applying c. 37.1-37.2 in R. 37, c. V.2)***

1199. The provisions described above apply equally to the fight against terrorism and TF.

***Timeliness to Requests for Provisional Measures including Confiscation (c. 38.1)***

1200. The German legal system relating to mutual legal assistance contains provisions which permit an effective and timely response to mutual legal assistance requests related to the identification, seizure, confiscation and forfeiture of laundered property and proceeds from, instrumentalities used in or instrumentalities intended for use in the commission of ML, TF or other predicate offenses.

1201. Pursuant to Section 66(1) of the LIACM, property (objects—*Gegenstände*) which the perpetrator or an accessory has acquired as a result of the offense forming the basis for the request for legal assistance or as payment for such property can be surrendered to another country. Property which the perpetrator or an accessory has received from the sale of an acquired object or as compensation for destroying, damaging, or withdrawing it or on the basis of an acquired right or from which profit has been drawn can be surrendered in accordance with Section 66 of the LIACM. The same applies to property deriving from the offense forming the basis for the request for legal assistance or which was needed or intended for the preparation or commission of the offense or to objects which emanated from the offense on which the request is based or was used or intended for use in its commission or preparation.

1202. Pursuant to Section 66(3) of the LIACM, surrender is only permissible as long as there is no final and enforceable foreign ruling in respect of the property. From this point onwards the provisions on execution assistance apply.

1203. The granting of execution assistance in cases of foreign decisions on confiscation and forfeiture is governed by the provisions of Section 48 et seq. of the LIACM. Pursuant to Section 48 second sentence of the LIACM, a foreign decision can be declared enforceable by virtue of an exequatur decision in respect of an order on forfeiture or an order on confiscation. The material prerequisites for this are regulated in Section 49 of the LIACM (existence of a request, enclosure of a final and enforceable court decision, observance of minimum procedural standards in the procedure of the requesting country, existence of dual criminality, no limitation under German law, no decision in Germany pursuant to Section 9 number 1 of the LIACM).

1204. If a final court exequatur decision exists, a decision on the granting of the request is taken by the responsible authority in accordance with Section 74 of the LIACM (see remark at 36. 3). Pursuant to Section 56(4) of the LIACM, the granting of a request for forfeiture or confiscation of property has the same effects described in Sections 73e, 74e of the CC, as if the decision would have been issued by a German court.

1205. Pursuant to Section 58(3) first sentence and Section 67(1) of the LIACM, the property that may be subject to forfeiture or confiscation may be seized or otherwise secured even prior to the receipt of the request by the foreign country and a search may also be conducted.

1206. Pursuant to Section 58(3) second sentence of the LIACM, and under the conditions specified in Section 66 subsection 2 numbers 1 and 2 of the LIACM, seizure mechanisms – such as an attachment *in rem* – can be executed upon request in preparation for a pending confiscation or forfeiture decision on the part of the requesting country. The decision may also involve property of corresponding value. A seizure mechanism of this kind prior to receipt of a formal request for enforcement is contingent upon adequate justification of the need for seizure. The seizure as such is undertaken in accordance with a decision made by the responsible German court pursuant to Sections 67 (1) first sentence, 77(1) of the LIACM and Sections 94 et seq. and 111b et seq. of the CPC.



1207. After the seizure has taken place and upon presentation of a legally effective ruling from the requesting country, confiscation or forfeiture (including for property of equivalent value) can be effected by means of enforcement assistance in accordance with Section 48 et seq. of the LIACM.

1208. With regards to relationships with other member states of the European Union, Council Framework Decision 2006/783/JHA of October 6, 2006 on the application of the principle of mutual recognition to confiscation orders requires changes in the German legal system in respect of mutual legal assistance. The act implementing the Framework Decision entered into force on October 22, 2009 (*i.e.* too late to be taken into account for the purpose of this assessment). The purpose of the Framework Decision is to improve cooperation in the execution of penal decisions leading to the final withdrawal of instrumentalities and the proceeds from crimes. An important innovation that would derive from implementation of this decision is that there would no longer be a need to verify the existence of dual criminality, provided one of the categories of offense listed in the Framework Decision applies. Pursuant to Section 6 (1) of the Framework Decision, this would include ML offenses.

1209. It should be noted, however, that the deficiencies in the ML offense described under Recommendation 1 may impact on Germany's ability to provide mutual legal assistance where dual criminality is a precondition, especially for non-EU jurisdictions. Such impact may likely be limited given the exceptional circumstances where dual criminality is required and the lack of unduly restrictive requirements. Despite the lack of statistics, the authorities have assured assessors that no requests for MLA have ever been denied by Germany, or rejected by other countries upon a request by Germany, on the basis of dual criminality requirements not being met because of the deficiencies in the ML offense.

1210. Finally, the limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by professional privileges (*i.e.* lawyers and notaries) may limit Germany's ability to deliver mutual legal assistance where such DNFBPs are involved.

#### ***Property of Corresponding Value (c. 38.2)***

1211. Pursuant to Section 49(1) Number 3 of the LIACM, enforcement assistance can be provided if a request is made for enforcement of an order for forfeiture or confiscation, provided an order of this kind could have been issued in accordance with German law. Accordingly, this would also cover requests related to property of corresponding value which, as described under Recommendation 3, are also contemplated under German law.

#### ***Coordination of Seizure and Confiscation Actions (c. 38.3)***

1212. Provisions for coordinating seizures and forfeiture or confiscation actions with other countries can be found in most of the bilateral and multilateral agreements that Germany has celebrated with other countries for the provision of mutual legal assistance.

1213. Moreover, Germany's Asset Recovery Office is a member of the European Camden Asset Recovery Inter-Agency Network (CARIN) and has undertaken commitments in connection with Council Decision 2007/845/JHA of December 6, 2007 concerning cooperation between Asset Recovery Offices of the member states in the field of tracing and identifying proceeds from, or other property related to, crime.

1214. Germany is also a member of the European Judicial Network (EJN) and sends one national member (and three assistant members) to Eurojust. Both institutions – Eurojust and the EJN – can be used for communication purposes and the coordination of criminal investigations in cross-border cases. Germany is represented at the EJN by the Federal Office of Justice, which exercises relevant responsibilities in mutual legal assistance and by representatives of the *Länder*.

***International Cooperation under SR V (applying c. 38.1-38.3 in R. 38, c. V.3)***

1215. The provisions described above apply equally to the fight against terrorism and TF.

***Asset Forfeiture Fund (c. 38.4)***

1216. Germany has considered establishing an asset forfeiture fund but has reached the decision that it is not necessary to establish such fund. In Germany, any funds identified, frozen, seized and confiscated are disbursed to the revenue authorities (Section 56 (4) of the LIACM in conjunction with Sections 73 lit. e and 74 lit. e of the CC (*Strafgesetzbuch*, StGB)). The exact use is provided for by Section 60 of the Ordinance on the Execution of Sentences (*Strafvollstreckungsordnung*, StVollstrO) which sets forth:

1217. “Upon the ruling becoming final and conclusive, ownership in the objects forfeited or seized shall devolve to that *Land* (judicial revenue authority) in which a court has handed down a ruling in the first stage of appeal. This shall apply also in those instances in which a ruling was handed down during the first stage of appeal by way of the jurisdiction of the Federation being exercised. If the court orders the objects to be forfeited or seized to the benefit of the Federation, the Federal Republic of Germany (judicial revenue authority) shall become the owner. Any rights of third parties shall remain unaffected (Section 73 e (1) second sentence, and 74 e (2), first sentence, of the CC (StGB)), unless the court has ordered their expiry (Section 74 e (2), second and third sentence of the CC). Should any rights have been forfeited or seized, sentences 1 through 4 shall apply *mutatis mutandis*.”

1218. With legislation transposing the Framework Decision on the application of the principle of mutual recognition to confiscation orders, which came into force on October 22, 2009, the pre-requisites are being created for facilitating, in the future, the surrender, in part, of assets to the requesting state that are identified, frozen, seized, and confiscated in the course of enforcement assistance.

***Sharing of Confiscated Assets (c. 38.5)***

1219. At the time of the on-site mission, Germany had considered a policy for the sharing of confiscated assets when confiscation is directly or indirectly a result of coordinated enforcement actions. It had drafted a bill to permit agreements with foreign countries with regards to sharing confiscated assets. That would, *inter alia*, reflect the obligation to share confiscated assets (subject to a *de minimis* threshold) mandated by the European Union Framework Decision on the application of the principle of mutual recognition to confiscation orders, referred to earlier. As mentioned above, the legislation came into force on October 22, 2009.

***Additional Element (R 38) – Recognition of Foreign Orders for a) Confiscation of assets from organizations principally criminal in nature; b) Civil forfeiture; and, c) Confiscation of Property which Reverses Burden of Proof (applying c. 3.7 in R.3, c. 38.6)***

1220. Foreign noncriminal confiscation orders would not be recognized or enforced in Germany. In accordance with Section 48, second sentence, of the LIACM, the provisions on execution assistance must be applied in response to a request for the enforcement of a forfeiture or confiscation order which a court in the requesting country has issued, provided the order is based on a punishable offense.

***Additional Element under SR V (applying c. 38.4-38.6 in R. 38, c V.7)***

1221. The provisions described above apply equally to the fight against terrorism and TF.

### ***Statistics (applying R.32)***

1222. Germany does not keep comprehensive statistics on mutual legal assistance with other countries. Only limited statistics were provided to the assessors. The authorities state that incoming and outgoing requests for mutual legal assistance are not reflected in statistics because: *i)* individual cases are not submitted to a central department. This is the result of the federal system of government given in Germany, and of the fact that in the interests of an enhanced efficiency in mutual legal assistance, responsibility was transferred from the federal government to the *Länder* and the local authorities. No legal basis exists for the federal government to place the *Länder* under obligation to keep statistics of such cases; *ii)* the number of requests for legal assistance filed by Germany with other countries and received by German authorities is immense. Their number is estimated at somewhere between 15 000 to 20 000 such requests per year. The staff and financial resources required to comprehensively capture such data in statistics are not available, and; *iii)* the purpose intended, which is to review the efficiency and quality with which such requests are processed, cannot be achieved by keeping such statistics.

1223. The authorities noted that no objections have been lodged by other countries, with which regular bilateral consultations and meetings take place in the various networks formed (such as the European Judicial Network, CARIN, Asset Recovery Offices, the prosecutors general of the Baltic Sea states), or by the European Union, the Council of Europe, the G8 nations and the United Nations, as regards any deficits that may have arisen in isolated cases. No concerns were received by the assessors from FATF or FSRB member countries.

1224. Notwithstanding the above, in the absence of comprehensive statistics, assessors were unable to fully evaluate the effectiveness of the system.

### **6.3.2. Recommendations and Comments**

1225. In order to comply fully with Recommendation 36, 37, 38, and Special Recommendation V, Germany should:

#### ***With respect to Recommendation 36***

- Address the deficiencies in the ML offense, noted under Recommendation 1, which may impact on the ability of Germany to provide certain forms of international cooperation where dual criminality is required.
- Remove the limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by professional privileges (i.e., lawyers and notaries) as such limitations may limit Germany's ability to deliver mutual legal assistance where such DNFBPs are involved.
- Maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of the mutual legal assistance system (such as requests that are made or received, relating to ML, the predicate offenses, and TF, including the nature of the request, whether it was granted or refused, and the time required to respond).

#### ***With respect to Recommendation 37***

- Remove the limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by professional privileges (*i.e.* lawyers and

notaries) as such limitations may limit Germany's ability to deliver mutual legal assistance where such DNFBPs are involved.

- Maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of the mutual legal assistance system (such as requests that are made or received, relating to ML, the predicate offenses and TF, including the nature of the request, whether it was granted or refused, and the time required to respond).

#### ***With respect to Recommendation 38***

- Address the deficiencies in the ML offense noted under Recommendation 1 which may impact on the ability of Germany to provide certain forms of international cooperation where dual criminality is required.
- Remove the limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by professional privileges (*i.e.* lawyers and notaries) as such limitations may limit Germany's ability to deliver mutual legal assistance where such DNFBPs are involved.
- Maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of the mutual legal assistance system (such as requests that are made or received, relating to ML, the predicate offenses and TF, including the nature of the request, whether it was granted or refused, and the time required to respond).

#### ***With respect to Special Recommendation V***

- Maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of the mutual legal assistance system (such as requests that are made or received, relating to TF, including the nature of the request, whether it was granted or refused, and the time required to respond).

#### **6.3.3. Compliance with Recommendations 36 to 38 and Special Recommendation V**

	<b>Rating</b>	<b>Summary of factors relevant to s.6.3 underlying overall rating</b>
<b>R.36</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Ability to cooperate may be limited by the deficiencies in the ML offense under certain, likely limited, circumstances.</li> <li>• Professional secrecy is interpreted broadly by the liberal professions, and limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by it that may hinder effective cooperation.</li> <li>• Effectiveness could not be established (lack of comprehensive statistics).</li> </ul>
<b>R.37</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Professional secrecy is interpreted broadly by the liberal professions, and limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by it may hinder effective cooperation.</li> <li>• Effectiveness could not be established (lack of comprehensive statistics).</li> </ul>
<b>R.38</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Ability to cooperate limited by the deficiencies in the ML offense under certain, likely limited, circumstances.</li> <li>• Professional secrecy is interpreted broadly by the liberal professions, and limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by it may hinder effective cooperation.</li> <li>• Effectiveness could not be established (lack of comprehensive statistics).</li> </ul>

SR.V	LC	• Effectiveness could not be established (lack of comprehensive statistics).
------	----	--

#### 6.4. Extradition (R.37, 39, SR.V)

##### 6.4.1. Description and Analysis

###### *Legal Framework*

1226. Extradition in Germany is mainly regulated by the LIACM, the Guidelines, which were revised with effect from January 1, 2009, the international conventions to which Germany is a party, and by other multilateral and bilateral agreements concluded.

###### *Dual Criminality and Mutual Assistance (c. 37.1 & 37.2)*

1227. Dual criminality is a requirement for the provision of extradition. Pursuant to Section 3 Number 1 of the LIACM, extradition shall be granted, if the act contains the elements of a criminal offense under German law or if, after analogous conversion of the facts, the act would constitute an offense under German law.

1228. However, in accordance with Section 81 Number 4 of the LIACM, which implements the Framework Decision on the European Arrest Warrant, dated June 13, 2002 (RBEuHB), dual criminality does not need to be verified among EU member states, provided that, under the law of the requesting state, the act forming the basis of the request infringes a penal provision relating to the categories of offenses listed under Article 2 paragraph 2 of such Framework Decision (which includes ML).

###### *Money Laundering as Extraditable offense (c. 39.1)*

1229. ML is an extraditable offense in Germany. Extradition for the purposes of law enforcement and execution of sentences is governed in Germany by Section 3 of the LIACM.

1230. As stated above, pursuant to Section 3 number 1 of the LIACM, extradition shall be granted, if the act contains the elements of a criminal offense under German law or if, after analogous conversion of the facts, the act would constitute an offense under German law. It should be noted that the deficiencies of the ML offense identified under Recommendation 1 impact on Germany's ability to extradite.

1231. At the European Union level, pursuant to the Framework Decision of June 13, 2002 on the European Arrest Warrant and the surrender procedure between the member states, dual criminality is not subject to verification provided that the offense is a listed offense, which is the case for the ML offense.

1232. Pursuant to Section 3 subsection 2 of the LIACM, the extradition of a person to a foreign country for the purpose of law enforcement is permissible if the offense is punishable under German law by a maximum of at least one year of imprisonment or if, after analogous conversion of the facts, the act would, under German law, be punishable by such a penalty. The German offense of ML, therefore, qualifies as an extraditable offense under Section 3 of the LIACM as, pursuant to Section 261 of the CC, its basic form is punished with imprisonment from three months to five years.

###### *Extradition of Nationals (c. 39.2)*

1233. Article 16(2) second sentence of the Basic Law prohibits the extradition of German nationals. Exceptions may nevertheless be provided for by law to enable the extradition of Germans to another

member state of the EU or to an international court, provided that the rule of law is upheld (same provision of the Basic Law). The German legislative authority has made use of this authorization in the case of Section 80 of the LIACM, which implements the Framework Decision on the European Arrest Warrant of July 20, 2006.

1234. If extradition is ruled out on the grounds of nationality, criminal prosecution is undertaken in Germany on the basis of the principle of mandatory prosecution (established under Sections 152(2), 160, and 163 of the CPC). Pursuant to Section 7(2) of the CC, German law applies to other acts which were committed abroad if the act is punishable at the place of its commission, or the place of its commission is subject to no criminal law enforcement, and if the perpetrator was a German at the time of the act or became one after the act. No specific request to prosecute would be necessary from the country seeking extradition.

***Cooperation for Prosecution of Nationals (applying c. 39.2(b), c. 39.3)***

1235. Cooperation between German authorities and foreign authorities is ensured on the basis of bilateral and multilateral treaties, but also through non-treaty-based judicial assistance, as described under Recommendation 36.

***Efficiency of Extradition Process (c. 39.4)***

1236. Pursuant to Number 19 subsection 1 of the Guidelines, requests for extradition and other requests for judicial assistance must be brought for authorization “without undue delay.” While the Guidelines do not state that the actual decision on authorization or refusal must be issued without delay, the authorities have confirmed that authorizations are granted fairly rapidly.

***Additional Element (R. 39) – Existence of Simplified Procedures relating to Extradition (c. 39.5)***

1237. The channels of communication to be used with other countries are usually set out in the individual bilateral treaties. In treaty-based extradition, there are usually extensive provisions for direct dealings (member states of the European Union) or for dealings undertaken via the Federal Ministry of Justice (extradition on the basis of the 1957 European Convention on Extradition (EuAIÜbk) or bilateral extradition agreements).

1238. For non-treaty-based judicial assistance, the LIACM allows for simplified extradition, provided the accused, after being advised of his rights, consents to such simplified extradition and his consent has been made part of the court record (Section 41 subsection 1 of the LIACM).

1239. For extraditions to other member states of the European Union, there are simplified procedures in the Framework Decision on the European Arrest Warrant, which was implemented in Germany through Section 79 et seq. of the LIACM.

***Additional Element under SR V (applying c. 39.5 in R. 39, c V.8)***

1240. The provisions described above apply equally to the fight against terrorism and TF.

***Statistics (applying R. 32):***

1241. The following table provides information on the amount of extradition requests received from other countries relating to ML, the amount of requests granted and the amount of requests denied.



Statistical Table 33: Extradition Requests from Other Countries

	Requesting State (& date of request)	Offenses	Request pending	Request granted (& date of response)	Request denied (& date of response)
<b>2005</b>	Austria (17.02.2005)	ML			X (27.07.2005)
	Russian Federation (31.03.2005)	ML		X (06.09.2005)	
	France (17.05.2005)	ML			X (22.04.2008)
	Switzerland (15.04.2005)	ML		X (09.06.2005)	
	Switzerland (15.04.2005)	ML		X (09.06.2005)	
	France (27.07.2005)	ML		X (28.11.2005)	
Sub-totals	<b>6</b>			<b>4</b>	<b>2</b>
<b>2006</b>	Netherlands (08.02.2006)	ML		X (06.03.2006)	
	Portugal (04.04.2006)	ML			X (08.07.2008)
	Ukraine (19.04.2006)	ML		X (25.07.2006)	
	France (21.04.2006)	ML		X (31.05.2006)	
	Belgium (17.05.2006)	ML		X (24.08.2006)	
	France (03.07.2006)	ML		X (28.06.2006)	
	Poland (05.07.2006)	ML		X (13.02.2007)	
	Peru (18.09.2006)	ML		X (19.03.2008)	
	Belgium (03.10.2006)	ML		X (18.12.2006)	
	Belgium (10.10.2006)	ML		X (09.11.2006)	
	USA (21.12.2006)	ML		X (25.04.2007)	
Sub-totals	<b>11</b>			<b>10</b>	<b>1</b>
<b>2007</b>	Belgium (07.02.2007)	ML		X (14.05.2007)	

	Requesting State (& date of request)	Offenses	Request pending	Request granted (& date of response)	Request denied (& date of response)
	Greece (07.03.2007)	ML			X (18.01.2008)
	Slovenia (07.09.2007)	ML		X (19.09.2007)	
	Belgium (11.10.2007)	ML			X (16.01.2008)
	Netherlands (15.10.2007)	ML		X (27.12.2007)	
Sub-totals	<b>5</b>			<b>3</b>	<b>2</b>
<b>2008</b>	Italy (30.01.2008)	ML		X (18.02.2008)	
	Poland (05.03.2008)	ML		X (14.03.2008)	
	Switzerland (02.06.2008)	ML		X (13.10.2008)	
	USA (03.06.2008)	ML		X (14.08.2008)	
	Spain (05.06.2008)	ML		X (.....2009)	
	France (10.06.2008)	ML			X (11.08.2008)
	Spain (18.06.2008)	ML		X (22.08.2008)	
	Poland (24.06.2008)	ML		X (17.07.2008)	
	Netherlands (24.08.2008)	ML		X (16.07.2008)	
	Belgium (10.09.2008)	ML		X (06.03.2009)	
Sub-totals	<b>10</b>		<b>0</b>	<b>9</b>	<b>1</b>
<b>Totals</b>	<b>32</b>		<b>0</b>	<b>26</b>	<b>6</b>

### *Analysis of Effectiveness*

1242. Germany has shown that it has in place a solid system of extraditions. As the statistics reflect, in the last four years, Germany received 32 requests for extradition from 15 different countries (including countries from outside the EU). Germany has granted 25 of such requests, denied 6, and is still processing 1. The average time taken to grant an extradition request has been approximately three months.

1243. Given that dual criminality is a requirement for extraditions, the deficiencies in the ML offense noted under Recommendation 1 may have an impact on Germany's ability to provide extraditions. Such impact may likely be limited given the exceptional circumstances where dual criminality is required, and the lack of unduly restrictive requirements. The authorities have assured assessors that they are not aware of any requests for extradition that have been denied by Germany, or rejected by other countries upon a request by Germany, on the basis of dual criminality requirements not being met because of the deficiencies in the ML offense.

#### **6.4.2. Recommendations and Comments**

1244. In order to comply fully with Recommendation 37, 39, and Special Recommendation V, Germany should:

- Address the deficiencies in the ML offense, noted under Recommendation 1, which may impact on the ability of Germany to provide certain forms of international cooperation where dual criminality is required, such as extraditions, particularly for countries outside the EU.

#### **6.4.3. Compliance with Recommendations 37 & 39, and Special Recommendation V**

	<b>Rating</b>	<b>Summary of factors relevant to s.6.4 underlying overall rating</b>
<b>R.39</b>	<b>LC</b>	• Ability to grant extradition limited by the deficiencies in the ML offense.
<b>R.37</b>	<b>LC</b>	Rating for this section: <b>C</b>
<b>SR.V</b>	<b>LC</b>	Rating for this section: <b>C</b>

### **6.5. Other Forms of International Cooperation (R.40 & SR.V)**

#### **6.5.1. Description and Analysis**

##### **Legal Framework:**

##### **Cooperation between law enforcement agencies:**

1245. Germany has concluded bilateral security cooperation agreements with a large number of countries. These agreements govern the cooperation between security authorities in the prevention and prosecution of serious crimes, including ML and TF. These agreements lay the ground for an exchange of information on past and planned crimes, the exchange of personal data, the coordination and execution of operational measures, and the dispatch of liaison officers.

1246. The tasks and powers of the BKA are set out in the Federal Criminal Police Office Act (BKAG–*Bundeskriminalamtgesetz*). In combination with other federal law provisions, this act forms the legal basis for the work of the BKA in the context of international cooperation.

##### **Widest Range of International Cooperation (c. 40.1)**

1247. Pursuant to the Federal Criminal Police Office Act, German law enforcement agencies are able to provide some forms of international cooperation to their foreign counterparts outside the MLA framework. Most of the cooperation refers to the transmission of data in accordance with Section 14 of the Federal

Criminal Police Office Act, and also includes establishing identities, gathering information from registers, files and other databases, or delivering expert forensic opinions.

1248. As the national central police authority, the BKA has the main responsibilities relating to international police cooperation and is responsible, in particular, for the exchange of information with the responsible authorities of other countries that is needed to prevent and prosecute crime. The BKA is the national central bureau of the International Criminal Police Organization (Interpol), the national office for Europol, and the central Schengen Office (Section 3 of the Federal Criminal Police Office Act). It is responsible for official relations required in the prevention or prosecution of criminal offenses between the Federal and *Länder* police and the police and judicial authorities and other competent public bodies in other countries.

1249. Pursuant to Section 3 subsection 3 of the Federal Criminal Police Office Act, the *Länder* police may, by way of an exception to the central authority principle, maintain direct official relations with the competent authorities in neighboring countries and with the member states of the European Union insofar as they refer to criminality which is of regional significance in border areas or insofar as there is an imminent danger. The *Länder* must inform the BKA without undue delay of such official relations.

***Provision of Assistance in Timely, Constructive and Effective Manner (c. 40.1.1):***

1250. As the national central authority, the BKA holds the central receiving point, the police operations and coordination center, which inspects and verifies all foreign requests and decides the responses on a case-by-case basis. Every *Land* has set up a central office (*Land* Criminal Police Office), which coordinates with the BKA. The *Land* Criminal Police Office is in charge of making sure that requests are delivered to the relevant local office. The Police Operations and Coordination Centre of the BKA has access to all the central police databases and functions as a 24-hour service center guaranteeing the immediate handling of urgent requests as well as the provision of information outside normal working hours (including with other countries).

1251. According to the authorities, this structure facilitates immediate processing of incoming foreign requests. However, in the absence of statistics, assessors were unable to evaluate the effectiveness of the system in this area.

***Clear and Effective Gateways for Exchange of Information (c. 40.2):***

1252. In the field of international police cooperation, the police authorities can use various channels of communication (including Interpol, Europol, common facilities with the littoral states in the border areas, liaison officers, etc.). According to the authorities, the most efficient channel is selected on a case-by-case basis.

***Spontaneous Exchange of Information (c. 40.3):***

1253. Germany has entered into a large number of bilateral and multilateral agreements which regulate spontaneous exchanges of information among law enforcement agencies on a bilateral basis.

1254. For cooperation among members of the EU, pursuant to Article 7 of the EU's Framework Decision, information and intelligence can be provided by law enforcement agencies, without the need for any prior request, in cases where there are factual reasons to believe that the information and intelligence could assist in the detection, prevention, or resolution of a concluding catalogue of offenses (among which ML is included).

***Making Inquiries on Behalf of Foreign Counterparts (c. 40.4):***

1255. No information was provided with respect to the ability of law enforcement agencies to conduct inquiries on behalf of foreign counterparts outside the MLA process.

***Conducting of Investigations on Behalf of Foreign Counterparts (c. 40.5):***

1256. No information was provided with respect to the ability of law enforcement agencies to conduct investigations on behalf of foreign counterparts outside the MLA process.

***No Unreasonable or Unduly Restrictive Conditions on Exchange of Information (c. 40.6):***

1257. Pursuant to Section 14 subsection 7 of the Federal Criminal Police Office Act, the recipient of personal data must be informed that the data transmitted may only be used by the recipient country for the purpose for which it was made available. In addition, personal data shall not be transferred where there is reason to assume that they would violate the objective of a German law (*i.e.* the abolition of capital punishment under Article 102 of Basic Constitutional Law). Further, data shall not be transferred if this would impair the interests of the data subject warranting protection, especially if an appropriate standard of data protection would not be guaranteed in the recipient country. The recipient country is also informed of the time in which the data transmitted must be deleted.

1258. The exchange of (personal) data under bilateral security agreements is also subject to strict conditions. The data transmitted may only be used for the purpose described in the respective agreement and only under the conditions specified by the transmitting party. Furthermore, the agreements contain detailed provisions on the documentation of the data exchange, data protection, the rights of inspection and indemnification for data subjects, and maximum retention periods.

***Provision of Assistance Regardless of Possible Involvement of Fiscal Matters (c. 40.7):***

1259. Pursuant to the bilateral security agreements, the sole involvement with fiscal matters is not considered to be a reason for rejecting cooperation.

***Provision of Assistance Regardless of Existence of Secrecy and Confidentiality Laws (c. 40.8):***

1260. The limitations of German law enforcement agencies in obtaining information protected by professional secrecy rules from certain DNFBPs (*i.e.* lawyers and notaries) may hinder Germany's ability to provide cooperation.

***Safeguards in Use of Exchanged Information (c. 40.9):***

1261. See 40.6 above.

***Additional Element – Exchange of Information with Non-Counterparts (c. 40.10 & c. 40.10.1):***

1262. No information was provided with respect to the ability of German law enforcement agencies to cooperate with non-counterparts.

***Additional Element – Provision of Information to FIU by Other Competent Authorities pursuant to request from Foreign FIU (c. 40.11)***

1263. N/A

**International Cooperation under SR V (applying c. 40.1-40.9 in R. 40, c. V.5):**

1264. The ability of law enforcement agencies to provide cooperation described above includes cooperation related with TF.

**Additional Element under SR V (applying c. 40.10-40.11 in R. 40, c. V.9):**

1265. The ability of law enforcement agencies to provide cooperation described above includes cooperation related with TF.

**Cooperation between FIUs**

1266. The FIU has full powers to cooperate with its foreign counterparts and does so regularly.

**Cooperation between supervisory authorities**

1267. The Banking Act and the Insurance Supervisory Act regulate the possibility for the BaFin to cooperate with foreign authorities in the supervision of banks, financial services institutions, and insurance companies.

1268. The supervisors of the DNFBPs are not structurally organized to cooperate directly with their foreign counterparts. As a practical matter, professional secrecy obligations would pose significant impediments to sharing of information directly or indirectly with foreign counterparts.

**Widest Range of International Cooperation (c. 40.1)**

1269. The BaFin may cooperate on banking supervision, insurance and securities and supervision of groups of institutions, or financial holding groups of issues. It applies the following provisions to cooperate: Sections 8 and 9(1) *a contrario* of the Banking Act, 84(4) *a contrario* of the Insurance Supervisory Act and 7 and 8(1) *a contrario* of the Securities Trading Act).

1270. Cooperation on banking prudential supervisory issues with counterparts from other states of the European Economic Area (EEA) is based on Section 8 of the Banking Act. Cooperation on AML/CFT issues can be provided on the basis of Section 9(1) of the Banking Act, regardless of whether or not the foreign counterpart is from an EU or EAA state.

1271. Pursuant to Section 8 of the Banking Act, communications with the competent authorities of the other EEA state may solely be used for the following purposes:

- For checking an institution's license to conduct business,
- For monitoring the operations of institutions on an individual basis or a consolidated basis,
- For directives (*Anordnungen*) issued by the BaFin and for the prosecution and punishment by the BaFin of administrative offenses (*Ordnungswidrigkeiten*),
- In the context of administrative proceedings regarding legal remedies against a decision by the BaFin, or
- In the context of proceedings before administrative courts, insolvency courts, public prosecutors' offices, or courts having jurisdiction in criminal cases or administrative fine cases.



1272. Information held by the BaFin may be passed on to:

- Public prosecutors' offices or courts having jurisdiction in criminal cases and administrative fine cases,
- Authorities entrusted with the supervision of institutions, collective investment companies, financial enterprises, insurance enterprises, the financial markets or the payments system, and to persons commissioned by such authorities,
- Authorities dealing with an institution's liquidation or the initiation of insolvency proceedings over its assets,
- Persons entrusted with the statutory auditing of the accounts of institutions or financial enterprises and to authorities which supervise such persons,
- A deposit guarantee scheme or an investor compensation scheme,
- Stock markets or financial futures exchanges, or
- Central banks.

Insofar as these authorities require the information for the performance of their functions (Section 9 of the Banking Act *a contrario*).

1273. As mentioned above, international cooperation is rendered possible by the Insurance Supervisory Act (Section 84(4) sentence 3 *a contrario*) on issues related to supervision of insurance companies, and by the Securities Trading Act on issues related to securities trading supervision (Sections 7 and 8 (1) sentence 5 *a contrario*).

1274. The BaFin may also cooperate on issues related to the supervision of financial conglomerates<sup>79</sup> on the basis of Section 8a of the Banking Act and Section 104 lit.1 of the Insurance Supervisory Act.

1275. The BaFin also frequently cooperates with the supervisory authorities and FIUs in other countries if it wants to issue licenses for the conducting of money remittance services to persons resident in another country. In such cases, it makes enquiries with the authorities in another country whether any information is held there to be said against the issue of a license.

1276. In all the instances above, the cooperation that the BaFin may provide is subject to the general pre-conditions that the requesting foreign authorities and the persons are subject to confidentiality requirement corresponding to those applicable to the BaFin staff, and that the information is solely used for the purpose for which it has been forwarded. Information which comes from another state may only be forwarded with the explicit consent of the competent authorities which have communicated this information and may only be passed on for the purposes these authorities have consented to. In this

---

<sup>79</sup> Financial conglomerates as provided in the Directive 2002/87/EC of the European Parliament and of the Council of December 16, 2002 on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate and amending Council Directives 73/239/EEC, 79/267/EEC, 92/49/EEC, 92/96/EEC, 93/6/EEC and 93/22/EEC, and Directives 98/78/EC and 2000/12/EC of the European Parliament and of the Council (OJ EC 2003 No. L 35, p. 1.)

context, it is also permissible to answer informal inquiries and to hand out documents as a matter of principle

***Provision of Assistance in Timely, Constructive and Effective Manner (c. 40.1.1):***

1277. The gateways mentioned above enable the BaFin to cooperate in a rapid, constructive, and effective manner with its foreign counterparts.

***Clear and Effective Gateways for Exchange of Information (c. 40.2):***

1278. In several cases, the BaFin has concluded Memoranda of Understanding (MoUs) with supervisory authorities of foreign states concerning their cooperation in the field of financial supervision which allow them inter alia to inspect German branches and subsidiaries of financial institutions domiciled in their states on site in their capacity as home-country authority. Since 1999, these MoU also contain a special paragraph with regard to financial crimes, i.e. ML, if the foreign authority has responsibility also with regard to AML/CFT. As of 2007, the BaFin had concluded 96 MoUs with financial supervisory authorities, as illustrated in the following table:

**The BaFin Memoranda of Understanding (as of 2007)<sup>80</sup>**

<b>Banking Supervisory Dept. (BA)</b>		<b>Securities Supervisory Dept. (WA)</b>		<b>Insurance Supervisory Dept. (VA)</b>	
Argentina	2001	Argentina	1998	Australia	2005
Australia	2005	Australia	1998	Canada	2004
Austria	2000	Austria	2000	China	2001
Belgium	1993	Brazil	1999	Croatia	2008
Brazil	2006	Canada	2003	Czech Rep	2002
Canada	2004	China	1998	Dubai	2006
China	2004	Croatia	2008	Estonia	2002
Croatia	2008	Cyprus	2003	Hong Kong SAR	2008
Czech Rep	2003	Czech Rep	1998	Hungary	2002
Denmark	1993	Dubai	2006	Korea	2006
Dubai	2006	France	1996	Latvia	2001
Estonia	2002	Hong Kong SAR	1998	Lithuania	2003
Finland	1995	Hungary	1998	Malta	2004
France	1992	Italy	1997	Qatar	2008
Greece	1993	Jersey	2001	Romania	2004
Hong Kong SAR(2)	1997	Luxembourg	2004	Slovakia	2001
Hungary	2000	Poland	1999	USA (4)	2007
Ireland	1993	Portugal	1998		
Italy	1993	Qatar	2008		
Jersey	2000	Russia	2001		
Korea	2001	Singapore	2000		
Latvia	2000	Slovakia	2004		
Lithuania	2001	South Africa	2001		
Luxembourg	1993	Spain	1997		
Malta	2004	Taiwan POC	1997		
Netherlands	1993	Turkey	2000		
Norway	1995	UAE	2008		
Philippines	2007	USA (3)	1997		
Poland	2008				
Portugal	1996				
Qatar	2008				
Romania	2003				
Russia	2006				
Sweden	1995				
Slovakia	2003				
Slovenia	2001				
South Africa	2004				
Spain	1993				
UK	1995				
USA (6)	2003				

<sup>80</sup> Numbers in brackets are number of agencies where there is an MOU with more than one authority. In these cases, the year refers to the first year that an MOU was established with that country.

***Spontaneous Exchange of Information (c. 40.3):***

1279. As mentioned above, it is possible for the BaFin—particularly in the scope of combating ML and TF – to cooperate on an international level both “spontaneously” and “upon request” without any problem. This type of cooperation is possible in particular with both foreign supervisory authorities and foreign law enforcement authorities and FIUs. In contrast to many authorities in other countries, the BaFin can also work directly with those types of authorities that are not supervisory authorities. For further details see above under Criterion 40.1.

***Making Inquiries on Behalf of Foreign Counterparts (c. 40.4):***

1280. The BaFin is authorized to conduct inquiries on behalf of foreign supervisors as described under 40.1.

***Conducting of Investigations on Behalf of Foreign Counterparts (c. 40.5):***

1281. No information was provided.

***No Unreasonable or Unduly Restrictive Conditions on Exchange of Information (c. 40.6):***

1282. See write up under 40.1

***Provision of Assistance Regardless of Possible Involvement of Fiscal Matters (c. 40.7):***

1283. The fact that a request for cooperation may involve fiscal matters in itself is not a ground for the BaFin to refuse to cooperate.

***Provision of Assistance Regardless of Existence of Secrecy and Confidentiality Laws (c. 40.8):***

1284. There are no secrecy or confidentiality requirements that hinder the BaFin from providing the requested assistance.

***Safeguards in Use of Exchanged Information (c. 40.9):***

1285. See write up under 40.1

***Additional Element – Exchange of Information with Non-Counterparts (c. 40.10 & c. 40.10.1):***

1286. Assessors did not receive any information upon which to reach a conclusion on this issue.

***Additional Element – Provision of Information to FIU by Other Competent Authorities pursuant to request from Foreign FIU (c. 40.11)***

1287. Assessors did not receive any information upon which to reach a conclusion on this issue.

***International Cooperation under SR V (applying c. 40.1-40.9 in R. 40, c. V.5):***

1288. See above.

***Additional Element under SR V (applying c. 40.10-40.11 in R. 40, c. V.9):***

1289. See above.

**Statistics (applying R.32):**

1290. Statistics on international cooperation were available for the FIU and the BaFin. These are shown in Statistical Table 34.

**Statistical Table 34: FIU information exchanges**

2003	482
2004	606
2005	667
2006	737
2007	744

\*in 2007 the total number consisted of 653 enquiries from abroad and 91 German requests to other FIUs

\*\* 2007 Annual report notes exchanges took place with 71 foreign FIUs

\*\*\* Top 20 exchange partners accounted for 581/744 exchanges or 78% of total

Source: BKA Annual Reports 2004 - 2007

**Statistical Table 35: The BaFin Information Exchange**

	2004	2005	2006	2007	2008	2009
<b>Discussions and meetings</b>						
...with foreign supervisory Authorities	8	9	15	11	5	6
...with other foreign agencies	11	5	3	4	2	2
<b>Written correspondence</b> (including official notes, opinions and reports)						
...with foreign supervisory authorities	20	13	10	32	12	20
...with international bodies	19	12	17	23	20	13

**Analysis of Effectiveness**

1291. For the most part, the authorities are capable of and appear to be providing a wide range of international cooperation. The limitations noted elsewhere on the scope of the ML offense and the TF offense may in practice limit some types of cooperation. The assessors did not obtain statistics from all authorities, particularly those in the *Länder* and those responsible for DNFBPs. Accordingly; it is difficult for the assessors to make an overall assessment of how effective international cooperation is. The primary area where there is the greatest doubt about cooperation relates to the DNFBP sector.

**6.5.2 Recommendations and Comments**

1292. In order to comply fully with Recommendation 40, Germany should:

- Ensure that cooperation may be granted by supervisors of DNFBPs.
- Ensure that professional secrecy obligations of DNFBPs are not an undue obstacle to sharing of information directly or indirectly with foreign counterparts.
- Keep statistics on the extent of international cooperation by authorities other than the FIU and the BaFin.

### 6.5.3 Compliance with Recommendation 40 and Special Recommendation V

	Rating	Summary of factors relative to s.6.5 underlying overall rating
<b>R.40</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• The way that professional secrecy is interpreted by the liberal professions may limit ability to provide cooperation in all cases.</li> <li>• No statistics available to evaluate overall effectiveness of cooperation other than for the FIU and the BaFin.</li> </ul>
<b>SR.V</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Scope of TF offenses may limit ability to provide cooperation in all cases.</li> <li>• The way that professional secrecy is interpreted by the liberal professions may limit ability to provide cooperation in all cases.</li> <li>• No statistics available to evaluate overall effectiveness of cooperation.</li> </ul>



## 7. OTHER ISSUES

### 7.1. Resources and Statistics

	Rating	Summary of factors underlying rating
R.30	LC	<ul style="list-style-type: none"> <li>• The FIU function is inappropriately structured, with some FIU roles being carried out within the <i>Länder</i>.</li> <li>• Assessors were not able to assess the adequacy of resources of <i>Länder</i> police involved in ML and TF.</li> <li>• Inadequate resources for supervising insurance intermediaries and DNFBPs.</li> </ul>
R.32	PC	<ul style="list-style-type: none"> <li>• Assessors found no hard evidence of any national level efforts aimed at reviewing the effective implementation of Germany's AML/CFT regime.</li> <li>• Comprehensive annual statistics are not maintained, were not available, or both in relation to: <ul style="list-style-type: none"> <li>○ sanctions imposed for ML convictions;</li> <li>○ the number of STRs analyzed or disseminated;</li> <li>○ the value of transactions associated with STRs;</li> <li>○ provisional measures;</li> <li>○ ML investigations;</li> <li>○ reports filed on international wire transfers;</li> <li>○ the amount of property confiscated broken down in relation to ML, TF, and other criminal proceeds;</li> <li>○ international cooperation;</li> <li>○ the structure, activities, or both of the financial sector (including in relation to the number of foreign branches of domestic FIs), nor the DNFBP sector; and</li> <li>○ the exercise of supervisory powers in the DNFBP sector.</li> </ul> </li> </ul>

### 7.2. Other relevant AML/CFT Measures or Issues

#### *Automated Access to account data under section 24c of the Banking Act*

1293. In section 2.5 of this Report, the automated account access system controlled by the BaFin is referenced. The system (established to enable Germany to fulfill its obligations under the EC Mutual assistance protocol of 2001) is designed to allow the authorities to determine whether a particular person (natural or legal) has a bank account or a safe custody account (collectively, "accounts") with a German credit institution or a foreign credit institution with a branch in Germany.

1294. Banks and investment companies are required to record core data on each account (not transaction data, such as account balance, account volumes, etc.), and must ensure that the BaFin has

automated access to these core data at all times. Furthermore, banks must take technical and organizational measures to ensure that they cannot monitor data retrievals by the authorities.

1295. Core data is defined in Section 24c (1) of the Banking Act to mean:

- The account number;
- The dates on which the account was opened and closed;
- The names and dates of birth of account holders and persons authorized to dispose of an account;
- The name of a legal person that is an account holder or authorized to dispose of an account; and
- The name and, if possible, the address of any other beneficial owner as defined in Section 1 (6) of the AML Act.

The data has to be updated on a daily basis.

1296. The BaFin advised the assessors that the automated account access system enables the BaFin to speedily identify accounts which might be subject to freezing or other requirements under Section 6a of the Banking Act (see discussion under Section 2.4, above), to provide support for international pre-notification and notification of terrorist lists (nationally coordinated by the Federal Ministry of Economics and Technology) and the determination of accounts held by those under investigation for ML or TF offenses and to detect accounts that could be used for unauthorized money remittance activity. Under Section 24c of the Banking Act, the BaFin is responsible for managing the system and ensuring that all financial institutions create and record the necessary master files containing prescribed information. From the foregoing, it is readily apparent that the system is accessed mostly by law enforcement agencies. The BaFin itself only uses the system in limited circumstances.

1297. System access is limited to the BaFin, other financial market supervisory authorities, authorities responsible for international judicial assistance, the authority responsible for enforcing the Foreign Trade and Payments Act, the FIU and – in cases of criminal proceedings – several law enforcement agencies (e.g. police, public prosecutors, tax investigation units, customs authorities, and courts). The vast majority of access requests originate with the police, tax authorities, public prosecutors, customers' offices, and various other law enforcement authorities. For example, the BaFin only accessed the system for itself 277 times in 2008, compared to 416 times by the FIU, and 83 245 times by other authorities.

1298. In 2005, Germany established a second automated account access system under Section 93b of the Fiscal Code. Access to this system is controlled by the Federal Central Tax Office, not the BaFin. This access system is outside the scope of this assessment; however, both automated account access systems are operated through a collective interface provided by the Center for Information Processing and Information Technology at the MoF.

**Table 1. Ratings of Compliance with FATF Recommendations**

The rating of compliance vis-à-vis the FATF 40+ 9 Recommendations is made according to the four levels of compliance mentioned in the AML/CFT assessment Methodology 2004 (Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC)), or could, in exceptional cases, be marked as not applicable (N/A).

These ratings are based only on the essential criteria set out in the Methodology, and defined in the following table, which also shows how many ratings from each category Germany obtained:

Rating Label	Description	Germany
<b>Compliant (C)</b>	The Recommendation is fully observed with respect to all essential criteria.	5
<b>Largely compliant (LC)</b>	There are only minor shortcomings, with a large majority of the essential criteria being fully met.	24
<b>Partially compliant (PC)</b>	The country has taken some substantive action and complies with some of the essential criteria.	15
<b>Non-compliant (NC)</b>	There are major shortcomings, with a large majority of the essential criteria not being met.	5
<b>Not applicable (NA)</b>	A requirement or part of a requirement does not apply, due to the structural, legal or institutional features of a country e.g. a particular type of financial institution does not exist in that country.	0

Forty Recommendations	Rating	Summary of factors underlying rating <sup>81</sup>
<b>Legal systems</b>		
1. ML offense	<b>PC</b>	<ul style="list-style-type: none"> <li>• “Counterfeiting and piracy of products”, and “insider trading and market manipulation” are not predicate offenses to ML.</li> <li>• The ML offense cannot be applied to persons who commit and are convicted for the predicate offense. The inability to do this is not supported by principles that amount to fundamental principles under the FATF standards.</li> <li>• Issues of effectiveness: <ul style="list-style-type: none"> <li>○ The comparatively low level of sanctions for the offense and the burden of proof required to establish that proceeds relate to a predicate crime encourage the use of charges other than ML to pursue serious and organized crime or situations of third party ML.</li> <li>○ The restriction on applying the ML offense to persons who are convicted of the predicate offense tends to result in ML investigations being dropped in favor of investigations into the predicate offense.</li> </ul> </li> </ul>
2. ML offense—mental element and corporate liability	<b>LC</b>	<ul style="list-style-type: none"> <li>• Natural and legal persons are not subject to effective, proportionate and dissuasive sanctions for basic ML.</li> </ul>

<sup>81</sup> These factors are only required to be set out when the rating is less than Compliant.

Forty Recommendations	Rating	Summary of factors underlying rating <sup>81</sup>
		<ul style="list-style-type: none"> <li>• Due to the lack of statistics, assessors could not determine that sanctions are applied effectively to legal persons.</li> </ul>
3. Confiscation and provisional measures	<b>LC</b>	<ul style="list-style-type: none"> <li>• Professional secrecy is interpreted broadly by the liberal professions, and there are strict conditions for obtaining or compelling information subject to it, which hinder the possibility for law enforcement authorities to locate and trace property.</li> <li>• Assets actually forfeited or confiscated are low compared to the total value of assets subjected to orders for forfeiture or confiscation.</li> </ul>
<b>Preventive measures</b>		
4. Secrecy laws consistent with the Recommendations	<b>C</b>	This Recommendation is fully observed.
5. Customer due diligence	<b>PC</b>	<ul style="list-style-type: none"> <li>• Reasonable measures to verify beneficial ownership are not required in all cases.</li> <li>• Definition of beneficial ownership of a trust is incomplete.</li> <li>• Broad exemptions from CDD given for “low risk” customers without apparent risk assessment.</li> <li>• “Low risk” exemptions result in absence, in certain circumstances, of any obligation (i) to undertake ongoing monitoring of transactions and (ii) to undertake CDD when doubts arise about the veracity of existing customer identification.</li> <li>• No requirement to consider filing STR in case of failure to complete CDD.</li> <li>• No clear evidence of the overall level of implementation due to relatively recent enactment of new obligations.</li> </ul>
6. Politically-exposed persons	<b>PC</b>	<ul style="list-style-type: none"> <li>• No requirements with respect to PEPs when they are the beneficial owners of the contracting party.</li> <li>• Provisions do not apply to foreign PEPs residing in Germany.</li> <li>• Approval to commence or continue the business relationship is not specified to be at senior management level.</li> </ul>
7. Correspondent banking	<b>PC</b>	<ul style="list-style-type: none"> <li>• Special measures apply only to non-EU correspondent relationships.</li> <li>• Approval to commence the business relationship is not specified to be at senior management level.</li> </ul>
8. New technologies & non face-to-face business	<b>LC</b>	<ul style="list-style-type: none"> <li>• No specific obligation to take measures to prevent the misuse of technological developments.</li> </ul>
9. Third parties and introducers	<b>LC</b>	<ul style="list-style-type: none"> <li>• No national assessment of the suitability of the specified institutions and professions which may act as introducers.</li> </ul>

Forty Recommendations	Rating	Summary of factors underlying rating <sup>81</sup>
10. Record keeping	<b>LC</b>	<ul style="list-style-type: none"> <li>• Uncertainty about what information would be acquired (and therefore retained) on “low risk” customers.</li> </ul>
11. Unusual transactions	<b>PC</b>	<ul style="list-style-type: none"> <li>• Uncertainty about the ability of institutions to monitor statutory “low risk” customers effectively.</li> <li>• No obligation to record and retain an analysis of transactions that have no apparent or visible economic or lawful purpose.</li> </ul>
12. DNFBP–R.5, 6, 8–11	<b>NC</b>	<ul style="list-style-type: none"> <li>• No arrangements for casinos to link identification-on-entry data to individual transactions within the casino.</li> <li>• Low awareness of CDD obligations and ML vulnerability among real estate agents and no oversight of compliance with CDD obligations of real estate agents and dealers in precious metals and precious stones.</li> <li>• No arrangements to promote and ensure AML/CFT compliance by TCSPs.</li> <li>• Inadequate awareness of ML and TF risk by casino operators, real estate agents, lawyers, notaries and auditors; underdeveloped risk assessment procedures.</li> <li>• Registered legal advisers are not subject to professional secrecy, they should not be included in the carve-out for legal and professional privilege.</li> <li>• No requirements for procedures to identify PEPs, or to consider filing an STR in cases where CDD cannot be completed, or to establish beneficial ownership in all cases.</li> <li>• Professional secrecy provisions are interpreted broadly by the liberal professions, and pose a significant impediment to their ability to provide records as evidence for prosecution of a crime (as called for under c 10.1.1) or keep findings available for competent authorities (as called for under c. 11.3).</li> </ul>
13. Suspicious transaction reporting	<b>PC</b>	<ul style="list-style-type: none"> <li>• Scope of reporting relates to ML only and not to proceeds of criminal activity.</li> <li>• Threshold for reporting requires a high degree of certainty of an offense, and the report constitutes a criminal complaint.</li> <li>• Reporting obligation does not cover “insider dealing and market manipulation”, nor “counterfeiting and piracy of products” as these are not predicate offenses for ML.</li> <li>• Material deficiencies in the TF offense limit the reporting obligation.</li> <li>• High threshold for reporting creates the need for investigation which in turn makes prompt reporting of suspicions impracticable.</li> <li>• Low level of reporting suggests that not all aspects of the regime are working effectively.</li> </ul>

Forty Recommendations	Rating	Summary of factors underlying rating <sup>81</sup>
14. Protection & no tipping-off	<b>LC</b>	<ul style="list-style-type: none"> <li>• Tipping-off prohibition applies only to reports that have already been filed.</li> </ul>
15. Internal controls, compliance & audit	<b>PC</b>	<ul style="list-style-type: none"> <li>• The compliance officer measures do not apply to the insurance intermediaries sector.</li> <li>• No legal obligation to ensure that the compliance officer has timely access to relevant CDD information.</li> <li>• No obligation to provide training to staff other than those involved in dealing with customers or carrying out transactions.</li> <li>• No legal obligations imposed on financial institutions requiring them to put in place screening procedures to ensure high standards when hiring employees.</li> <li>• Application of measures across corporate groups is new and effectiveness could not be assessed.</li> </ul>
16. DNFBP–R.13–15 & 21	<b>NC</b>	<ul style="list-style-type: none"> <li>• No requirement to have compliance management arrangements.</li> <li>• Discretionary exemption of most professions from safeguards based on firm size but not risk of ML or TF.</li> <li>• No risk assessments to justify safeguards exemptions or simplified measures.</li> <li>• In absence of safeguards, no training requirement.</li> <li>• No requirement to screen to insure high standards when hiring.</li> <li>• No audit function for DNFBPs.</li> <li>• No specific requirement for casinos to have AML/CFT internal controls or to have an audit function.</li> <li>• No supervisory framework for real estate agents and dealers in precious metals and stones and, hence, no specific requirements for internal policies and controls and screening and audit.</li> <li>• Inadequate awareness of potential ML vulnerabilities contributing to underreporting.</li> <li>• Inadequate risk assessment procedures among professions, leading to inadequate monitoring and underreporting.</li> <li>• Broad carve-out for legal and professional privilege combined with strict professional secrecy requirements place significant impediments to STR reporting.</li> </ul>
17. Sanctions	<b>PC</b>	<ul style="list-style-type: none"> <li>• Administrative fines in place are not proportionate (very low number of administrative fines available under the AML Act) nor sufficiently dissuasive (more serious violations of the AML Act attract lower levels of administrative fines); and the maximum amounts of fines under the AML Act are low (especially considering the large size of many German financial institutions); and, due to the criminal nature of the penalties, high penalties can only be applied for gross negligence or deliberate intent).</li> </ul>



Forty Recommendations	Rating	Summary of factors underlying rating <sup>81</sup>
		<ul style="list-style-type: none"> <li>• Administrative fines are not applied effectively – the BaFin has only ever applied one administrative fine many years ago.</li> <li>• Due to the constitutional principle of specificity, there are no administrative fines for violations of obligations to establish appropriate internal safeguards under all sector-specific laws; and apply enhanced due diligence in specific additional circumstances listed in the Banking and Investment Acts.</li> <li>• Failure by the supervisory boards to comply with their obligation to supervise management may result in uncertainty as to whether administrative fines apply to individual members of such boards.</li> </ul>
18. Shell banks	<b>C</b>	<ul style="list-style-type: none"> <li>• This Recommendation is fully observed.</li> </ul>
19. Other forms of reporting	<b>C</b>	<ul style="list-style-type: none"> <li>• This Recommendation is fully observed.</li> </ul>
20. Other NFBP & secure transaction techniques	<b>C</b>	<ul style="list-style-type: none"> <li>• This recommendation is fully observed.</li> </ul>
21. Special attention for higher risk countries	<b>PC</b>	<ul style="list-style-type: none"> <li>• No explicit obligation to pay special attention to relationships and transactions involving countries with inadequate AML/CFT standards.</li> <li>• No obligation to record and retain an analysis of transactions that have no apparent or visible economic or lawful purpose.</li> </ul>
22. Foreign branches & subsidiaries	<b>LC</b>	<p>Scope limitations:</p> <ul style="list-style-type: none"> <li>• No measures which explicitly require financial institutions to pay particular attention to their branches and subsidiaries in EU or EEA member states that do not, or insufficiently, apply the FATF Recommendations</li> <li>• Obligation to notify authorities of inability to implement AML/CFT measures does not apply to EU or EEA financial institutions other than insurance undertakings.</li> </ul>
23. Regulation, supervision and monitoring	<b>LC</b>	<ul style="list-style-type: none"> <li>• Uncertainty about the legal basis for the BaFin's ability to apply fit and proper testing for members of supervisory boards of investment companies.</li> <li>• Lack of effectiveness in aspects of supervisory practice: <ul style="list-style-type: none"> <li>○ Lack of effective sanctions for non-compliance with AML/CFT requirements.</li> <li>○ Issues about uncertain quality of audit reports for some cooperative banks; AML/CFT auditing standard had not been updated.<sup>82</sup></li> <li>○ <i>Länder</i> authorities seem unfamiliar with their AML supervisory responsibilities and appear to apply insufficient resources to supervise a large</li> </ul> </li> </ul>

<sup>82</sup> Regulations were issued on November 26, 2009 to address this issue (albeit outside the 2 months timeframe mentioned in the FATF Handbook for countries and evaluators).

Forty Recommendations	Rating	Summary of factors underlying rating <sup>81</sup>
		<p>number of insurance intermediaries.</p> <ul style="list-style-type: none"> <li>○ Fit and proper requirements for supervisory board members have not been applied to existing board members due to the newness of the requirements.</li> </ul>
24. DNFBP—regulation, supervision and monitoring	<b>NC</b>	<ul style="list-style-type: none"> <li>• Inadequate supervisory authority and capacity with respect to oversight of real estate agents and persons trading in precious metals and stones.</li> <li>• Insufficient supervisory oversight of AML compliance by casino operators.</li> <li>• No authority for Chambers of Lawyers, Chamber of Patent Attorneys, and Chambers of Tax Advisors to conduct routine compliance monitoring of members.</li> <li>• Compliance monitoring and enforcement generally ineffective, including: <ul style="list-style-type: none"> <li>○ Lack of awareness of ML risks in casinos.</li> <li>○ Risk assessments have not been developed by the competent authorities responsible for monitoring and ensuring compliance with AML/CFT requirements.</li> </ul> </li> <li>• Insufficient resources and capacity for supervisors of real estate agents and dealers in precious metals and precious stones.</li> </ul>
25. Guidelines & Feedback	<b>PC</b>	<ul style="list-style-type: none"> <li>• Very poor specific feedback on STRs filed with the <i>Länder</i> authorities.</li> <li>• Uncertainty in some parts of the financial sector on the status of abrogated circulars.</li> <li>• New (replacement) private sector guidance (approved by the BaFin and the MoF) is limited in scope.</li> <li>• Lack of comprehensive guidance in place for the insurance intermediaries sector.</li> <li>• Guidelines for lawyers, auditors have not been updated, no guidelines for dealers in precious metals and stones and real estate agents.</li> </ul>
<b>Institutional and other measures</b>		
26. The FIU	<b>LC</b>	<ul style="list-style-type: none"> <li>• FIU is only one of many centers that receives, analyzes, and disseminates STRs and other relevant information concerning suspected ML or TF activities.</li> <li>• The FIU carries out limited case-specific analysis of STRs, and less than ten cases each year where that analysis is directed towards informing a decision about whether to disseminate information to domestic authorities for investigation on the basis that there are grounds to suspect ML or TF.</li> <li>• Overall effectiveness of the FIU function as expected under R.26 is or may be compromised by: <ul style="list-style-type: none"> <li>○ Guidance to reporting entities on form and manner of reporting is not sufficiently strong and information is received and accepted in a variety of</li> </ul> </li> </ul>

Forty Recommendations	Rating	Summary of factors underlying rating <sup>81</sup>
		<p>formats and through various channels.</p> <ul style="list-style-type: none"> <li>○ Data in STR attachments sent to LEAs are not always available to the FIU for entry into the FIU database and thus not always available for analysis.</li> <li>○ No information in FIU database about value of transactions in STRs.</li> <li>○ No ongoing national coordination or management of tactical analysis of STR information.</li> <li>○ Inability to produce statistics on STRs analyzed or disseminated or linked to a prosecution or conviction of ML and confiscation of proceeds.</li> </ul>
27. Law enforcement authorities	<b>LC</b>	<ul style="list-style-type: none"> <li>● The offense of ML is not being properly investigated. The focus is placed on self launderers with few investigations conducted into more complex organized ML structures.</li> <li>● The lack of complete statistics has prevented assessors from fully evaluating the effectiveness of this recommendation.</li> </ul>
28. Powers of competent authorities	<b>LC</b>	<ul style="list-style-type: none"> <li>● The lack of complete statistics has prevented assessors from fully evaluating the effectiveness of this recommendation.</li> </ul>
29. Supervisors	<b>LC</b>	<ul style="list-style-type: none"> <li>● Although the BaFin has adequate supervisory powers there are weaknesses in respect of the effective use of such powers in practice.</li> <li>● Fit and proper requirements for supervisory board members have not been applied to existing board members due to the newness of the requirements.</li> </ul>
30. Resources, integrity, and training	<b>LC</b>	<ul style="list-style-type: none"> <li>● The FIU function is inappropriately structured, with some FIU roles being carried out within the Länder.</li> <li>● Assessors were not able to assess the adequacy of resources of Länder police involved in ML and TF.</li> <li>● Inadequate resources for supervising insurance intermediaries and DNFBPs.</li> </ul>
31. National cooperation	<b>LC</b>	<ul style="list-style-type: none"> <li>● No effective coordination with authorities responsible for DNFBPs.</li> <li>● Policy co-ordination focuses primarily on FATF policy matters rather than developing policies and activities to combat ML and TF in Germany.</li> </ul>
32. Statistics	<b>PC</b>	<ul style="list-style-type: none"> <li>● No evidence that overall reviews of effectiveness of the German AML/CFT system have been undertaken.</li> <li>● Comprehensive annual statistics are not maintained, were not available, or both in relation to: <ul style="list-style-type: none"> <li>○ sanctions imposed for ML convictions;</li> <li>○ the number of STRs analyzed or disseminated;</li> <li>○ the value of transactions associated with STRs;</li> <li>○ provisional measures;</li> </ul> </li> </ul>

Forty Recommendations	Rating	Summary of factors underlying rating <sup>81</sup>
		<ul style="list-style-type: none"> <li>○ ML investigations;</li> <li>○ reports filed on international wire transfers;</li> <li>○ the amount of property confiscated broken down in relation to ML, TF, and other criminal proceeds;</li> <li>○ international cooperation;</li> <li>○ the structure, activities or both of the financial sector (including in relation to the number of foreign branches of domestic FIs), nor the DNFBP sector; and</li> <li>○ the exercise of supervisory powers in the DNFBP sector.</li> </ul>
33. Legal persons–beneficial owners	<b>NC</b>	<ul style="list-style-type: none"> <li>● No mechanisms in place to ensure in all cases access in a timely fashion to information on the control and beneficial ownership of legal entities other than publicly listed stock corporations.</li> <li>● Complete lack of transparency over stock corporations that issue their shares in bearer form, and over private foundations.</li> <li>● No risk assessment undertaken by the authorities to ascertain the risk of ML/TF in the case of joint stock companies which have issued bearer shares.</li> </ul>
34. Legal arrangements – beneficial owners	<b>NC</b>	<ul style="list-style-type: none"> <li>● Insufficient measures in place to ensure transparency over <i>Treuhand</i>.</li> </ul>
<b>International Cooperation</b>		
35. Conventions	<b>PC</b>	<p>Germany has not fully implemented the Palermo Convention:</p> <ul style="list-style-type: none"> <li>● The ML offense cannot be applied to persons who commit and are convicted for the predicate offense. The inability to do this is not supported by principles that amount to fundamental principles under the FATF standards.</li> <li>● “Insider trading and market manipulation”, and “counterfeiting and piracy of products” are not predicate offenses to ML.</li> <li>● Natural and legal persons are not subject to effective, proportionate and dissuasive sanctions for basic ML.</li> </ul>
36. Mutual legal assistance (MLA)	<b>LC</b>	<ul style="list-style-type: none"> <li>● Ability to cooperate may be limited by the deficiencies in the ML offense in certain, likely limited, circumstances.</li> <li>● Professional secrecy is interpreted broadly by the liberal professions, and limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by it that may hinder effective cooperation.</li> <li>● Effectiveness could not be assessed (lack of comprehensive statistics).</li> </ul>
37. Dual criminality	<b>LC</b>	<ul style="list-style-type: none"> <li>● Professional secrecy is interpreted broadly by the liberal professions, and limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by it may hinder effective cooperation.</li> </ul>

Forty Recommendations	Rating	Summary of factors underlying rating <sup>81</sup>
		<ul style="list-style-type: none"> <li>Effectiveness could not be assessed (lack of comprehensive statistics).</li> </ul>
38. MLA on confiscation and freezing	<b>LC</b>	<ul style="list-style-type: none"> <li>Ability to cooperate limited by the deficiencies in the ML offense under certain, likely limited, circumstances.</li> <li>Professional secrecy is interpreted broadly by the liberal professions, and limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by it may hinder effective cooperation.</li> <li>Effectiveness could not be assessed (lack of comprehensive statistics).</li> </ul>
39. Extradition	<b>LC</b>	<ul style="list-style-type: none"> <li>Ability to grant extradition limited by the deficiencies in the ML offense.</li> </ul>
40. Other forms of co-operation	<b>LC</b>	<ul style="list-style-type: none"> <li>The way that professional secrecy is interpreted by the liberal professions may limit ability to provide cooperation in all cases.</li> <li>No statistics available to evaluate overall effectiveness of cooperation other than for the FIU and the BaFin.</li> </ul>
<b>Nine Special Recommendations</b>		
SR.I Implement UN instruments	<b>PC</b>	<p>Germany has not fully implemented the Terrorism Financing Convention and the relevant UNSCR:</p> <ul style="list-style-type: none"> <li>The definition of “serious violent act endangering the state” is not fully consistent with the CFT Convention as it does not extend to all acts that constitute offenses within the scope of, and as defined in the treaties annexed to the CFT Convention and it does not cover serious bodily injuries.</li> <li>The definition of the term “funds” in connection with the financing of a terrorist act or individual terrorist is not fully in line with the requirements of the CFT Convention, as it imposes a requirement for the funds to be of a certain minimum value (i.e., not merely insubstantial).</li> <li>The financing to carry out a terrorist act and the financing of an individual terrorist are not fully consistent with the CFT Convention.</li> <li>Natural and legal persons are not subject to effective, proportionate and dissuasive sanctions.</li> <li>Except for credit institutions, financial services institutions and investment companies, no other person is subject to directly applicable requirements for the freezing of assets for EU-internals under S/RES/1373.</li> <li>Lack of effective procedures making it possible to freeze assets other than funds for EU-internals where the Banking Act applies.</li> <li>There are no appropriate measures to monitor effectively the compliance with freezing obligations by persons and entities other than financial institutions</li> </ul>

Forty Recommendations	Rating	Summary of factors underlying rating <sup>81</sup>
SR.II Criminalize terrorist financing	<b>LC</b>	<p>and “companies”.</p> <ul style="list-style-type: none"> <li>• The definition of “serious violent act endangering the state” is not fully consistent with SR II as it does not extend to all acts that constitute offenses within the scope of, and as defined in the treaties annexed to the Terrorist Financing Convention and it does not cover serious bodily injuries.</li> <li>• The definition of the term “funds” in connection with the financing of a terrorist act or individual terrorist is not fully in line with the requirements of SR II, as it imposes a requirement for the funds to be of a certain minimum value (i.e. not merely insubstantial).</li> <li>• The minimum level of sanctions raises the possibility that the sanctions imposed may not be effective, proportionate and dissuasive.</li> <li>• Effectiveness not established: lack of specific statistics.</li> </ul>
SR.III Freeze and confiscate terrorist assets	<b>PC</b>	<ul style="list-style-type: none"> <li>• Except for credit institutions, financial services institutions and investment companies, no other person is subject to directly applicable requirements for the freezing of assets for EU-internals under S/RES/1373.</li> <li>• Lack of effective procedures to freeze assets other than funds for EU-internals where the Banking Act applies.</li> <li>• Professional secrecy is interpreted broadly by the liberal professions, and there are strict conditions for obtaining or compelling information subject to it, which hinder the possibility for law enforcement authorities to locate and trace terrorist funds or other assets.</li> <li>• No appropriate measures to monitor effectively the compliance with obligations under SR.III by persons and entities other than financial institutions and “companies”.</li> </ul>
SR.IV Suspicious transaction reporting	<b>PC</b>	<ul style="list-style-type: none"> <li>• Threshold for reporting requires a high degree of certainty of an offense, and the report constitutes a criminal complaint.</li> <li>• Material deficiencies in the TF offense limit the reporting obligation.</li> <li>• High threshold for reporting makes prompt reporting of suspicions impracticable.</li> </ul>
SR.V International cooperation	<b>LC</b>	<p><b><i>In application of R 36-38:</i></b></p> <ul style="list-style-type: none"> <li>• Effectiveness could not be assessed (lack of comprehensive statistics).</li> </ul> <p><b><i>In application of R. 40:</i></b></p> <ul style="list-style-type: none"> <li>• Scope of TF offenses may limit ability to provide cooperation in all cases.</li> <li>• The way that professional secrecy is interpreted by the liberal professions may limit ability to provide cooperation in all cases.</li> </ul>



Forty Recommendations	Rating	Summary of factors underlying rating <sup>81</sup>
		<ul style="list-style-type: none"> <li>No statistics available to evaluate overall effectiveness of cooperation.</li> </ul>
SR.VI AML/CFT requirements for money/value transfer services	<b>LC</b>	<ul style="list-style-type: none"> <li>Effectiveness: deficiencies in regulations or other measures in the areas of CDD, reporting of suspicious transactions, and sanctions.</li> </ul>
SR.VII Wire transfer rules	<b>C</b>	This Recommendation is fully observed.
SR.VIII Nonprofit organizations	<b>LC</b>	<ul style="list-style-type: none"> <li>Review of NPO laws and regulations and on-going reassessments of vulnerabilities not documented.</li> <li>Data on NPOs available from association registration documents or from tax filings for tax benefit status is sparse relative to the financial information they are expected to hold under the Interpretative Note to SR VIII, Section 6 b, and the financial transparency Section of the 2002 FATF best practices paper and is of limited usefulness for monitoring individual organizations or for sectoral monitoring.</li> <li>Low intensity of outreach to raise awareness of TF risk in NPO sector, even within a strategy of safeguarding and maintaining the practice of charitable giving and the strong and diversified community of institutions through which it operates.</li> </ul>
SR.IX Cross-Border Declaration & Disclosure	<b>LC</b>	<ul style="list-style-type: none"> <li>Weakness in measures for alerting air travelers arriving in Germany from outside of the EU as to their declaration obligations.</li> <li>One-year period of retention of most data in the INZOLL database considerably diminishes the utility of that database for analysis.</li> </ul>

**Table 2. Recommended Action Plan to Improve the AML/CFT System**

FATF 40+9 Recommendations	Recommended Action (in order of priority within each section)
1. General	
2. Legal System and Related Institutional Measures	
2.1 Criminalization of Money Laundering (R.1 & 2)	<ul style="list-style-type: none"> <li>• Amend the CC to re-categorize the offense of ML as a serious crime and to raise the range of sanctions to make them effective, proportional and dissuasive, relative to other serious offenses in the CC.</li> <li>• Increasing the minimum and maximum ranges of sanctions applicable to ML, consistent with the level of penalties for serious offenses in Germany.</li> <li>• Reduce the burden of proof that is deemed necessary to prove that property is the proceeds of crime.</li> <li>• Create predicate offenses for ML for the following two categories of offenses: “insider trading and market manipulation” and “counterfeiting and piracy of products.”</li> <li>• Amend the CC to ensure that predicate offenses for ML include a range of offenses in each of the designated categories of offenses without having to meet the additional requirement (aggravating circumstances) that the offense is committed to make a profit, or by a member of a gang founded for the recurrent commission of such an offense.</li> <li>• Allow for the concurrent prosecution of and sanctioning for self laundering and for the commission of the predicate offense.</li> <li>• Raise awareness among prosecutors and law enforcement agencies on the opportunity that ML investigations and convictions represent to the general fight against organized crime.</li> <li>• Maintain statistics on the sanctions applied to legal persons.</li> </ul>
2.2 Criminalization of Terrorist Financing (SR.II)	<ul style="list-style-type: none"> <li>• Criminalize the financing of a terrorist act and of an individual terrorist consistent with Article 2 of the TF Convention.</li> <li>• Undertake actions (awareness raising or training) to increase the application of regulatory sanctions against legal persons.</li> <li>• Increase the minimum and maximum ranges of sanctions applicable to TF so that it is made a serious offense.</li> <li>• Maintain complete statistics on the amount of investigations, prosecutions and convictions for TF offences.</li> </ul>
2.3 Confiscation, freezing, and seizing of proceeds of crime (R.3)	<ul style="list-style-type: none"> <li>• Enable law enforcement authorities to obtain access to information about ownership of property held by DNFBPs who claim that information is protected by professional secrecy rules.</li> <li>• Improve performance for actually confiscating or forfeiting assets once courts order those assets be confiscated or forfeited.</li> <li>• Establish a mechanism to collect and keep statistics on provisional measures applied.</li> </ul>
2.4 Freezing of funds used for terrorist financing (SR.III)	<ul style="list-style-type: none"> <li>• Enact national legislation to implement fully Council Common Positions, No. 2001/930/CFSP and No. 2001/931/CFSP on the fight</li> </ul>

FATF 40+9 Recommendations	Recommended Action (in order of priority within each section)
	<p>against terrorism, which are also applicable to EU-residents.</p> <ul style="list-style-type: none"> <li>• Enact legislation to make S/RES/1373 applicable to any person (including persons other than credit institutions, financial services institutions and investment companies) for the freezing of assets concerning EU-internals.</li> <li>• Set up procedures within Germany that will ensure in all cases the freezing without delay of assets other than funds (such as immovable goods, companies and businesses and vehicles); for the case of EU-internals where the Banking Act applies.</li> <li>• Set up appropriate measures to monitor effectively the compliance with the obligations under SRIII by persons and entities other than financial institutions and “companies”.</li> </ul>
2.5 The Financial Intelligence Unit and its functions (R.26)	<ul style="list-style-type: none"> <li>• Strengthen the capacity of the FIU to act as a national centre for receiving, analyzing, and disseminating to law enforcement and other appropriate agencies financial information about suspected ML and TF, more consistent with the standard enunciated in R.26, in particular, by having the FIU carry out more robust analysis of STRs directed towards disseminating information to State Police when the FIU concludes that there are grounds to suspect ML or TF.</li> <li>• Strengthen the FIU's tactical analytic capacity through increased personnel and training.</li> <li>• Equip the FIU with the authority to provide direction to reporting entities as to the manner and form of reporting suspicious transactions to the FIU and implement a standardized, more automated reporting system for STRs.</li> </ul>
2.6 Law enforcement, prosecution and other competent authorities (R.27 & 28)	<ul style="list-style-type: none"> <li>• Make more use of special techniques when conducting investigations into ML.</li> <li>• Undertake actions (awareness raising or training) to improve the focus of ML investigations and the amount of investigations conducted into more complex organized crime ML structures.</li> <li>• Maintain complete statistics on the use of powers to conduct ML or TF investigations and prosecutions.</li> </ul>
2.7 Cross-Border Declaration & Disclosure (SR IX)	<ul style="list-style-type: none"> <li>• Take steps to heighten travelers' awareness of the declaration and disclosure requirements by making much more visible (and in multiple languages) the signage at ports of entry and exit alerting travelers to the requirement.</li> <li>• Extend the one-year period of retention of most data in the INZOLL database.</li> </ul>
3. Preventive Measures—Financial Institutions	
3.1 Risk of money laundering or terrorist financing	
3.2 Customer due diligence, including enhanced or reduced measures (R.5–8)	<p><b>With respect to Recommendation 5:</b></p> <ul style="list-style-type: none"> <li>• Clarify the obligation with respect to the verification of beneficial ownership to bring it in line with the FATF standard, which requires that reasonable measures be taken to verify such ownership in all cases, including low risk.</li> <li>• Extend the concept of beneficial ownership of trusts and <i>Treuhand</i> to</li> </ul>

FATF 40+9 Recommendations	Recommended Action (in order of priority within each section)
	<p>include the settlor and any additional parties who may have direct or indirect control over the administration of the trust.</p> <ul style="list-style-type: none"> <li>• Review the exemption for low-risk customers and transactions to ensure that: <ul style="list-style-type: none"> <li>– The types of counterparty and the countries of origin are based on an appropriate risk-assessment by the authorities;</li> <li>– There remains an absolute obligation to monitor business relationships with such customers on an ongoing basis, and to keep records and information up to date; and</li> <li>– The exemption does not apply to circumstances where an institution has doubts about the veracity of information in its possession.</li> </ul> </li> <li>• Require institutions to consider filing an STR in case of failure to complete CDD.</li> <li>• Review the timeframe (2-10 years) in which institutions are expected to apply the current CDD requirements to existing customers.</li> </ul> <p><b>With respect to Recommendation 6:</b></p> <ul style="list-style-type: none"> <li>• Introduce an explicit requirement that the enhanced due diligence requirements apply in the event that a PEP is the beneficial owner of the contracting party.</li> <li>• Redefine the concept of a PEP to ensure that it does not exclude foreign PEPs who are resident in Germany.</li> <li>• Require “senior level” approval for establishment (and continuation) of a business relationship with a PEP, rather than simply the next level of management.</li> </ul> <p><b>With respect to Recommendation 7:</b></p> <ul style="list-style-type: none"> <li>• Extend the special enhanced CDD measures to respondent banks within the European Union</li> <li>• Require “senior level” approval for establishment of a correspondent banking relationship, rather than simply the next level of management</li> </ul> <p><b>With respect to Recommendation 8:</b></p> <ul style="list-style-type: none"> <li>• Introduce a specific obligation to have measures in place to prevent the misuse of technological developments</li> </ul>
3.3 Third parties and introduced business (R.9)	<ul style="list-style-type: none"> <li>• Implement a procedure to review the range of third party introducers and the composition of the EU equivalence list to ensure that it accurately reflects the authorities’ own assessment of the risks.</li> </ul>
3.4 Financial institution secrecy or confidentiality (R.4)	None.
3.5 Record keeping and wire transfer rules (R.10 & SR.VII)	<ul style="list-style-type: none"> <li>• Consider the potential consequences of the “low-risk” exemptions for the retention of meaningful information that can be made available to the competent authorities.</li> </ul>
3.6 Monitoring of transactions and relationships (R.11 & 21)	<p><b>With respect to Recommendation 11</b></p> <ul style="list-style-type: none"> <li>• Introduce an explicit requirement that a written analysis should be undertaken, and recorded (for a period of at least five years), of all complex, unusually large transactions and unusual patterns of transactions that have no apparent economic or lawful purpose.</li> </ul>

FATF 40+9 Recommendations	Recommended Action (in order of priority within each section)
	<ul style="list-style-type: none"> <li>• Clarify what procedures are expected with respect to “statutory” low-risk customers.</li> </ul> <p><b>With respect to Recommendation 21</b></p> <ul style="list-style-type: none"> <li>• Require institutions to pay special attention to business relationships and transactions with persons from or in jurisdictions that do not sufficiently apply the FATF standard, employing their own risk analyses, in addition to placing reliance on the circulars issued by the BaFin.</li> <li>• Introduce an explicit requirement that a written analysis should be undertaken, and recorded, of all such transactions.</li> </ul>
3.7 Suspicious transaction reports and other reporting (R.13, 14, 19, 25, & SR.IV)	<p><b>With respect to Recommendation 13 and Special Recommendation IV</b></p> <ul style="list-style-type: none"> <li>• Establish clearly that the legal threshold for STR reporting is an obligation with respect to transactions where the institution suspects or has reasonable grounds to suspect that the transaction involves the proceeds of crime.</li> <li>• Investigate the reasons for the exceptionally low level of reporting among certain institutions.</li> </ul> <p><b>With respect to Recommendation 14</b></p> <ul style="list-style-type: none"> <li>• Extend the tipping-off provision to cover cases where transactions are being reviewed internally to determine whether an STR should be filed.</li> </ul> <p><b>With respect to Recommendation 25</b></p> <ul style="list-style-type: none"> <li>• Discuss with the state prosecution authorities the introduction of a common approach to providing feedback to reporting institutions on both the overall quality of reports and their value in terms of investigations and prosecutions.</li> </ul>
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)	<p><b>With respect to Recommendation 15:</b></p> <ul style="list-style-type: none"> <li>• Ensure that the compliance officer is required to have timely access to relevant CDD information.</li> <li>• Introduce enforceable measures requiring financial entities to provide AML/CFT training to all staff; to require that employees be kept informed of new developments including information on current ML and TF techniques, methods and trends; and to require that there is a clear explanation of all aspects of AML/CFT and suspicious transaction reporting.</li> <li>• Introduce enforceable measures requiring financial institutions to apply screening procedures at the time of hiring all staff.</li> </ul> <p><b>With respect to Recommendation 22:</b></p> <ul style="list-style-type: none"> <li>• Introduce enforceable measures requiring all financial institutions to pay particular attention to branches and subsidiaries in countries that do not, or insufficiently, apply the FATF Recommendations;</li> <li>• Ensure that the provisions of section 25g of the Banking Act apply to subsidiaries and branches located in EEA and EU states;</li> <li>• Ensure that uniform standards are applied in the three principal sectors (banking, insurance and investment firms);</li> <li>• Implement an enforceable obligation for banks and investment firms to inform German supervisory authorities immediately when a foreign branch or subsidiary (including those in EEA states) is unable to</li> </ul>

FATF 40+9 Recommendations	Recommended Action (in order of priority within each section)
	observe appropriate AML/CFT measures.
3.9 Shell banks (R.18)	None
<p>3.10 The supervisory and oversight system—competent authorities and SROs</p> <p>Role, functions, duties and powers (including sanctions) (R.23, 29, 17 &amp; 25)</p>	<ul style="list-style-type: none"> <li>• Add specific administrative fines for AML violations into the Insurance Supervision Act and the Investment Act.</li> <li>• Increase the range of specific administrative fines under the AML Act and also lower application thresholds (negligence or deliberate intent).</li> <li>• Increase the amounts of specific administrative fines under the AML Act for the more serious violations set out in Section 17(2) of the AML Act, and extend their applicability to gross negligence.</li> <li>• Ensure that members of the (supervisory) Board of Directors are explicitly subject to appropriate administrative fines for failure to supervise managers responsible for compliance.</li> <li>• Introduce legal provisions that explicitly allow the BaFin to dismiss managers and members of (supervisory) Boards of Directors for AML/CFT violations.</li> <li>• Review the adequacy of the frequency with which the high-risk institutions are subject to on-site inspection by the BaFin and the consequential impact on resources.</li> <li>• Address the issue of guidance on audit report quality as a priority with the auditing organizations in the cooperative banking sector.</li> <li>• Ensure that <i>Länder</i> authorities are sufficiently aware of their AML/CFT supervisory responsibilities and apply sufficient resources to supervise insurance intermediaries.</li> <li>• Arrange for <i>Länder</i> authorities to issue guidance to insurance intermediaries.</li> </ul>
3.11 Money value transfer services (SR.VI)	<ul style="list-style-type: none"> <li>• The recommendations and comments applicable to Recommendations 5, 13, and 17 apply, where applicable, to the MVTS sector in accordance with the FATF methodology.</li> <li>• The authorities should consider applying more resources to identifying and closing illicit money remittance operations.</li> </ul>
4. Preventive Measures—Nonfinancial Businesses and Professions	
4.1 Customer due diligence and record-keeping (R.12)	<ul style="list-style-type: none"> <li>• Casinos should be required to adopt policies and procedure to link individual transactions to identified clients.</li> <li>• DNFBPs should be required to have procedures for identifying PEPs.</li> <li>• The recommended actions in Section 3 above with respect to R 5, 6, 9-11 should be implemented for DNFBPs, including, in particular, the need for a requirement to consider filing an STR in case of failure to complete CDD and for verification of beneficial ownership in all cases.</li> <li>• Registered legal advisers, who are not subject to the same statutory professional secrecy obligations as the other liberal professions, should be excluded from the carve-out for legal and professional privilege.</li> <li>• For full compliance with the Recommendations, the carve-out for legal and professional secrecy should generally be limited to information (a) obtained in the course of ascertaining the legal position of a client, or (b) in performing their task of defending or representing that client in or concerning judicial, administrative, arbitration, or mediation proceedings.</li> </ul>



FATF 40+9 Recommendations	Recommended Action (in order of priority within each section)
	<ul style="list-style-type: none"> <li>• Implementation               <ul style="list-style-type: none"> <li>○ Arrangements should be put in place to monitor and ensure CDD compliance by TCSPs; and routine CDD compliance monitoring should be strengthened by the authorities responsible for overseeing compliance by real estate agents, dealers in precious metals and dealers in precious stones, lawyers, auditors, accountants, and tax advisors.</li> <li>○ Outreach and Awareness raising                   <ul style="list-style-type: none"> <li>▪ The authorities should develop outreach campaigns specifically to raise awareness of CDD obligations of real estate agents and dealers in precious metals and precious stones and, more generally to raise awareness of ML and TF risks in all of the DNBFP sectors.</li> </ul> </li> <li>○ Training                   <ul style="list-style-type: none"> <li>▪ Casino staff and managers should be given additional training in ML techniques and risks.</li> <li>▪ CDD training requirements for real estate agents and dealers in precious metals and dealer in precious stones should be implemented</li> <li>▪ CDD training programs for lawyers, notaries and auditors should be intensified.</li> </ul> </li> </ul> </li> </ul>
4.2 Suspicious transaction reporting (R.16)	<ul style="list-style-type: none"> <li>• DNFBPs should be required to have some form of risk based compliance management arrangements.</li> <li>• The authorities should undertake a systematic assessment of the ML and TF vulnerability of the DNFBP sectors.</li> <li>• Authorities should develop programs to raise DNFBP's awareness of AML/CFT risks and improve DNFBP's ability to identify and report suspicious activities.</li> <li>• Exemptions from the safeguards requirements of the AML Act, or blanket simplified procedures, should be based on evaluation of ML and TF risk.</li> <li>• All DNFBPs should be subject to requirements to screen new hires for high standards, to train staff, and to have an AML/CFT audit function.</li> <li>• All casinos, real estate agents, and dealers in precious metals and stones should be required to have AML/CFT internal controls.</li> <li>• Authorities should review the scope of the carve-out from legal and professional privilege and the stringency of professional secrecy requirements with a view to permitting the professions to play a more forthcoming role in reporting of suspicious transactions.</li> </ul>
4.3 Regulation, supervision, monitoring, and sanctions (R.17, 24, & 25)	<ul style="list-style-type: none"> <li>• Clarify <i>Länder</i>-level AML/CFT supervisory responsibility for real estate agents and persons trading in goods and ensure adequate resources and capacity to carry out these responsibilities.</li> <li>• Strengthen AML/CFT supervisory capacity of casino supervisors.</li> <li>• Take steps to insure that Chambers of Lawyers, the Chamber of Patent Lawyers, and Chambers of Tax Advisors have adequate authority to conduct routine AML/CFT compliance monitor of their members.</li> <li>• Authorities should issue up-to-date guidance for all DNFBPs.</li> <li>• Authorities should carry out AML/CFT risk assessments of the various DNFBP sectors, maintain them up to date, and make sectors aware of risks.</li> </ul>
4.4 Other designated non- financial businesses and professions (R.20)	None.

FATF 40+9 Recommendations	Recommended Action (in order of priority within each section)
5. Legal Persons and Arrangements & Nonprofit Organizations	
5.1 Legal Persons—Access to beneficial ownership and control information (R.33)	<ul style="list-style-type: none"> <li>• Ensure that beneficial ownership on all types of legal entities is made accessible to the competent authorities.</li> <li>• Assess the risk of ML and TF posed by not publicly-listed companies that issue bearer shares and take necessary measures to mitigate the risk.</li> </ul>
5.2 Legal Arrangements—Access to beneficial ownership and control information (R.34)	<ul style="list-style-type: none"> <li>• Enhance transparency over <i>Treuhands</i>.</li> </ul>
5.3 Nonprofit organizations (SR.VIII)	<ul style="list-style-type: none"> <li>• Document that NPO laws and regulations have been systematically reviewed and updated and that the vulnerability of the NPO sector is periodically reassessed.</li> <li>• Require NPOs in their registration documents or in their filings for tax benefits to provide the information called for under Interpretative Note to SR VIII, Section 6 b and the financial transparency section of the 2002 FATF best practices paper.</li> <li>• Energize outreach efforts to maintain awareness of TF risk in NPO sector.</li> </ul>
6. National and International Cooperation	
6.1 National cooperation and coordination (R.31)	<ul style="list-style-type: none"> <li>• Ensure that the ML Contact Group meetings include a focus on national implementation of Germany's AML/CFT regime.</li> <li>• Put in place formal mechanisms to review the effectiveness of Germany's AML/CFT system.</li> <li>• Fully engage authorities responsible for DNFBPs.</li> <li>• Have the FIU provide the BaFin with information about the quality of STRs received from reporting entities.</li> <li>• Put in place formal mechanisms to enhance dialogue with the private sector.</li> <li>• Provide more resources to the MoF for it to coordinate national implementation.</li> </ul>
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)	<p><b>With respect to Recommendation 35:</b></p> <ul style="list-style-type: none"> <li>• Fully implement the Palermo Convention by criminalizing self-laundering.</li> <li>• Fully implement the Palermo Convention by making “insider trading and market manipulation” and “counterfeiting and piracy of products” predicate offenses for ML, amending the CC to ensure that predicate offenses for ML include a range of offenses in each of the designated categories of offenses without having to meet the additional requirement that the offense is committed with the intention to make a profit or by a member of a gang founded for the recurrent commission of such an offense, and increasing the minimum and maximum ranges consistent with the level of penalties for other serious offenses in Germany.</li> </ul>

FATF 40+9 Recommendations	Recommended Action (in order of priority within each section)
	<p><b>With respect to Special Recommendation I:</b></p> <ul style="list-style-type: none"> <li>• Fully implement the CFT Convention by amending Section 89a of the CC to extend the financing of a terrorist act and of an individual terrorist to all acts that constitute offenses within the scope of, and as defined in the treaties annexed to the CFT Convention, to cover serious bodily injuries, and to eliminate the requirement for the “funds” to be of a certain minimum value (i.e. not merely insubstantial).</li> <li>• Enact legislation to make S/RES/1373 applicable to any entity or persons other than credit institutions, financial services institutions and investment companies for the freezing of assets concerning EU-internals.</li> <li>• Set up procedures within Germany that will ensure in all cases the freezing without delay of assets other than funds (such as immovable goods, companies and businesses and vehicles) for cases of EU-internals where the Banking Act applies.</li> <li>• Set up appropriate measures to monitor effectively the compliance with freezing obligations by persons and entities other than financial institutions and “companies”.</li> </ul>
6.3 Mutual Legal Assistance (R.36, 37, 38 & SR.V)	<p><b>With respect to Recommendation 36:</b></p> <ul style="list-style-type: none"> <li>• Address the deficiencies in the ML offense, noted under Recommendation 1, which may impact on the ability of Germany to provide certain forms of international cooperation where dual criminality is required.</li> <li>• Remove the limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by professional privileges (i.e., lawyers and notaries) as such limitations may limit Germany’s ability to deliver mutual legal assistance where such DNFBPs are involved.</li> <li>• Maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of the mutual legal assistance system (such as requests that are made or received, relating to ML, the predicate offenses, and TF, including the nature of the request, whether it was granted or refused, and the time required to respond).</li> </ul> <p><b>With respect to Recommendation 37:</b></p> <ul style="list-style-type: none"> <li>• Remove the limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by professional privileges (i.e., lawyers and notaries) as such limitations may limit Germany’s ability to deliver mutual legal assistance where such DNFBPs are involved.</li> <li>• Maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of the mutual legal assistance system (such as requests that are made or received, relating to ML, the predicate offenses and TF, including the nature of the request, whether it was granted or refused, and the time required to respond).</li> </ul> <p><b>With respect to Recommendation 38:</b></p> <ul style="list-style-type: none"> <li>• Address the deficiencies in the ML offense noted under Recommendation 1 which may impact on the ability of Germany to provide certain forms of international cooperation where dual</li> </ul>

FATF 40+9 Recommendations	Recommended Action (in order of priority within each section)
	<p>criminality is required.</p> <ul style="list-style-type: none"> <li>• Remove the limitations faced by law enforcement agencies and prosecutors in obtaining documents and information from DNFBPs protected by professional privileges (i.e., lawyers and notaries) as such limitations may limit Germany's ability to deliver mutual legal assistance where such DNFBPs are involved.</li> <li>• Maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of the mutual legal assistance system (such as requests that are made or received, relating to ML, the predicate offenses and TF, including the nature of the request, whether it was granted or refused, and the time required to respond).</li> </ul> <p><b>With respect to Special Recommendation V:</b></p> <ul style="list-style-type: none"> <li>• Maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of the mutual legal assistance system (such as requests that are made or received, relating to TF, including the nature of the request, whether it was granted or refused, and the time required to respond).</li> </ul>
6.4 Extradition (R. 39, 37 & SR.V)	<ul style="list-style-type: none"> <li>• Address the deficiencies in the ML offense, noted under Recommendation 1, which may impact on the ability of Germany to provide certain forms of international cooperation where dual criminality is required, such as extraditions, particularly for countries outside the EU.</li> </ul>
6.5 Other Forms of Cooperation (R. 40 & SR.V)	<ul style="list-style-type: none"> <li>• Ensure that cooperation may be granted by supervisors of DNFBPs.</li> <li>• Ensure that professional secrecy obligations on DNFBPs are not an undue obstacle to sharing of information directly or indirectly with foreign counterparts.</li> <li>• Keep statistics on the extent of international cooperation by authorities other than the FIU and the BaFin.</li> </ul>
7. Other Issues	
7.1 Resources and statistics (R. 30 & 32)	
7.2 Other relevant AML/CFT measures or issues	
7.3 General framework – structural issues	

## ANNEX 1. DETAILS OF ALL BODIES MET DURING THE ON-SITE VISIT

List of ministries, other government authorities or bodies, private sector representatives and others.

### **Federal and Local (*Länder*) Authorities**

Federal Ministry of Economics

Federal Ministry of Finance

Federal Ministry of Foreign Affairs

Federal Ministry of Justice

Federal Ministry of the Interior

Ministry of Interior and Sports of the State Hesse

### **Criminal Justice and Operational Agencies**

Asset recovery office (MOJ)

Asset Recovery Offices

Customs Criminal Office

Customs Investigation Service

Federal and *Länder* judges

Federal and *Länder* prosecutors

Federal Criminal Police Office (BKA)

Federal Customs Administration

Federal Intelligence Service (BND)

Federal Office for the Protection of the Constitution

Federal Office of Economics and Export Control

Federal Office of Justice

Financial Intelligence Unit (FIU)

Joint Counter-terrorism Centre

Public Prosecutor's Office – Confiscation agency

State Bureaus of Criminal Investigation

### **Financial and Non-Financial Sector Supervisory Bodies**

Central Bank

Federal Financial Supervisory Authority, BaFin

Casino supervisory authority for the *Länder*

### **Private Sector Bodies**

Association of Public Banks (*Verband öffentlicher Banken–VÖB*)

Berlin Bar Association

Berlin Chamber of Notaries

Berlin Chamber of Tax Advisers

Central Association of the German Banking Industry (*Zentraler Kreditausschuss; ZKA*)

Chamber of Public Accountants

Chambers of Patent Attorneys

Federal Association of Credit Unions and Credit Cooperative Banks (*Bundesverband der Volksbanken und Raiffeisenbanken–BVR*)

Federal Association of German Banks (*Bundesverband deutscher Banken–BdB*)

Federal Bar Association

Federal Chamber of Tax Advisers

German Insurance Association (*Gesamtverband der Versicherungswirtschaft; GDV*)

German Insurance Association–GDV

### **Private Sector Representatives**

Academics

Audit Firms

Banks

Casinos

Dealers in precious metals/stones

Insurance companies

Lawyers

Money remitters

Notaries

Patent Attorneys

Public Accountants

Real estate agents

Tax advisers



**ANNEX 2. LIST OF ALL LAWS, REGULATIONS, AND OTHER MATERIAL RECEIVED**

<b>European legislation</b>
3L3 Common Understanding of the obligations imposed by European Regulation 1781/2006
Commission Directive 2006/70/EC of 1 August 2006
Commission regulation (EC) No 1330/2008 of 22 December 2008 amending for the 103rd time Council Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban
Council Regulation (EC) No 1110/2008 of 10 November 2008 amending Regulation (EC) No 423/2007 concerning restrictive measures against Iran
Council Regulation (EC) No 423/2007 of 19 April 2007 concerning restrictive measures against Iran
Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing
Directive 2007/64/EC on payment services in the internal market, i.e. "Payment Services Directive"
EU common understanding on the criteria for the recognition of third countries equivalence under the 3rd EU Anti-Money Laundering Directive
European Union's Regulation 1781/2006
Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism
Regulation (EC) 2580/2001 freezing funds of suspected terrorists
Regulation (EC) 881/2002 implementing UN Al Qai'da and Taliban sanctions
Regulation (EC) No 1889/2005 of The European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds
Regulation (EC) No 1889/2005 of The European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community
Third EC Money Laundering Directive
<b>Laws</b>
Act Governing Private Associations ( <i>Gesetz zur Regelung de öffentlichen Vereinsrechts</i> (VereinsG).
Act on Control of Weapons of War

Act on Suppression of Illegal Drug Trafficking and other Manifestations of Organized Crime
Act on the Federal Intelligence Service ( <i>Bundesnachrichtendienstgesetz</i> )
Act on the Prosecution of the Preparation of Serious Violent Acts Endangering the State ( <i>Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten, GVVG</i> )
Act Regulating the Co-operation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution ( <i>Bundesverfassungsschutzgesetz, BVerfSchG</i> )
Act Supplementing the Act to Fight Money Laundering and Terrorist Financing ( <i>Geldwäschebekämpfungsergänzungsgesetz, GwBekErG; AML Act</i> )
Act Supplementing the Counter-Terrorism Act
Administrative Offense Act
Asylum Procedure Act
Banking Act ( <i>Bankwesengesetz, BWG</i> )
Basic Law ( <i>Grundgesetz, GG</i> )
Civil Code ( <i>Bürgerliches Gesetzbuch, BGB</i> )
Civil Procedure Code
Commercial Code
Criminal Code
Criminal Procedures Code (CPC)
Customs Administration Act (CAA)
Customs Investigation Service Act
Digital Signature Act
Disciplinary Statute for lawyers and lawyer-candidates ( <i>Disziplinarstatut</i> )
Disciplinary Statute for lawyers and lawyer-candidates ( <i>Disziplinarstatut</i> )
Federal Criminal Police Office Act
Federal Statute on Auditors
Federal Statute on Lawyers
Federal Statute on Notaries
Federal Statute on Patent Attorneys
Fiscal Code ( <i>Abgabenordnung, AO</i> )

Foreign Trade and Payments Act (FTP)
Framework Decision on Confiscation has been implemented through a legislative act adopted on September 19, 2009 and which entered into force on October 22, 2009
Gambling Code for Public Gambling Casinos in Hesse - Excerpt
Gambling Treaty 2008
Hessian Gambling Casino Act- Excerpt
Insurance Contracts Act
Insurance Supervisory Act
Investment Act
Judicature Act ( <i>Gerichtsverfassungsgesetz</i> )
Law governing BND
Law on International Assistance in Criminal Matters (LIACM) ( <i>Gesetz über die internationale Rechtshilfe in Strafsachen IRG</i> )
Law on the Protection of the Constitution (BVerfSchG)
Legal Services Act (LSA)
Narcotics Law
Precursors Control Law
Public Accountant Act (WPO)
Regulation for the International Cooperation in Criminal Matters
Residence Act
Securities Deposit Act
Securities Trading Act (WpHG)
Selection of <i>Länder</i> casino acts
Selection of <i>Länder</i> Laws on Police
Stock Corporation Act ( <i>Aktiengesetz, AktG</i> )
Tax Consulting Act
Trade Law
Trade Regulations Act ( <i>GewO</i> )
Weapon Law

<b>Ordinances and Regulations</b>
Auditors Report Regulation for Credit Institutions and Financial Services Institutions
Digital Signature Ordinance
Fiscal Code Application Ordinance
Ordinance on the Execution of Sentences ( <i>Strafvollstreckungsordnung, StVollstrO</i> )
<b>Guidance</b>
<b>BaFin</b>
BaFin 1 Circular 8/2005 (GW): -Internal implementation of appropriate risk management systems for the prevention of money laundering, the financing of terrorism and fraud at the expense of institutions pursuant to sec. 25a (1), sentence 3, No. 6, and (1a) of the Banking Act and sec. 14 (2), No. 2, of the Money Laundering Act
BaFin 2 Circular 1/2003 -Further counter-measures against Ukraine -No further counter-measures against Nigeria - Maintenance of counter-measures against the Republic of Nauru
BaFin 3 Circular 10/2003 FATF list of non-cooperative countries and territories (Myanmar)
BaFin 4 Circular 4/2008 -FATF Statement of 28 February 2008 on Uzbekistan and the northern part of Cyprus as well as other countries and territories -Publication of a German translation of the FATF Typologies Report on "New Payment Methods"
BaFin 5 Circular 7/2008 -Countries and territories with equivalent requirements to combat money laundering and terrorist financing -German translation of the FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing of June 2007
BaFin 6 Circular 2/2009 (GW) Repeal/Declaration of lapse of Announcements, Circulars and individual letters
BaFin 7 Annex: Circulars that have been repealed or declared to have lapsed
BaFin 8 Circular Anti-money-laundering safeguards at credit institutions acting as correspondent banks
BaFin 9 Circular 8/2002 Safeguards to prevent money laundering in correspondent bank relations with credit institutions in the so-called Trans-Dniester Republic of Moldova
BaFin 10 Circular 15/2002 -Implementing of institutions' internal anti-money-laundering systems in the light of the decision on non-cooperative countries and territories taken at the FATF plenary session held on 21 June 2002: enhancing the worldwide effectiveness of anti-money-laundering measures -Further countermeasures against the

Republic of Nauru
BaFin 11 Circular 14/01 FATF list of non-cooperative countries and territories (Nauru)
BaFin 12 Circular 13/2008 (GW) Statement by the FATF dated 16 October 2008 regarding Uzbekistan and Iran
BaFin 13 Circular 25/2002 Internal implementation of anti-money laundering systems pursuant to section 25a (1) no. 4 of the German Banking Act ( <i>Kreditwesengesetz – KWG</i> ) and section 14 (2) no. 2 of the German Money Laundering Act
BaFin 14 Circular 8/2007 FATF Statement of 11 October 2007 on Iran
BaFin 15 Requirements for the granting of a licence to provide money transmission services pursuant to section 1 (1a) sentence 2 no. 6 of the German Banking Act
BaFin 16 Guidelines of the Federal Banking Supervisory Office of 30 March 1998 concerning measures to be taken by financial services institutions to combat and prevent money laundering
BaFin 17 Guidelines of the Federal Banking Supervisory Office of 30 March 1998 concerning measures to be taken by credit institutions to combat and prevent money laundering
BaFin 18 BaFin Letter to the Institut der Wirtschaftsprüferin Deutschland e.V. (IDW): Dispensability of IT research systems at smaller institutions 8 November 2008
BaFin 19 BaFin, Circular 4/98
BaFin Circular 2/2009
BaFin 20 Circular R 6/97
BaFin Circular 14/2009 of July 30, 2009
BaFin Circular 7/2008
ZKA guidelines ZKA Guidelines for the interpretation and application of the Act Supplementing the Act to Fight Money Laundering and Terrorist Financing
BaFin Compendium of letters sent to individual financial institutions ( <i>Consbruch</i> )
Notice on the granting of authorisation to provide financial services pursuant to section 32 (1) of the Germany Banking Act from 1 November 2007)
<b>Central Bank</b>
Circular 45/2008
Circular of 23 December 2008 on SR III
Instructions for notifications in the case of queries concerning legal acts imposing financial sanctions

<b>FIU</b>
Annual reports from 2004 to 2008
Guidance on Possible money laundering indications in accordance with section 261 of the Criminal Code relevant to newly obliged parties for professional groups pursuant to section 3(1) numbers 1 and 2 of the Money Laundering Act
Selection of FIUNewsletters
<b>Other</b>
Codes of Conduct applying to tax, customs, police, prosecutor's office
Federal Lawyers' Code
General Terms and Conditions of Business for Banks (GTCB for Banks) issued by the five banking associations for their members, and approved by the Federal Cartel Office
General Terms and Conditions of Business of several banks
Guidelines for auditors for the interpretation of the Money Laundering Act
Guidelines for Criminal Proceedings and Proceedings to Impose a Regulatory Fine ( <i>Richtlinien für das Strafverfahren und das Bußgeldverfahren, RiStBV</i> )
Lawyers Rules of Professional Practice
Ministry of Economics and Technology Circular of 02 December 2008 on SR III
Ministry of Economics and Technology Circular on Sanctions – new developments
Ministry of Economics and Technology Obligation of landlords under the EC regulations on combating terrorism
Order of the Federal Chamber of Lawyers pursuant to section 9 (4), second sentence, of the Act to Combat Money Laundering
Typology Paper for the Revenue Administration for reporting suspected cases of money laundering in accordance with Section 31 b of the AO (Fiscal Code) in conjunction with Section 261 of the StGB
Various court decisions with regard to principle of guilt, nulla poena sine culpa / predicate offence / committed on a commercial basis etc.



## **Copies of Key Laws, Regulations, and Other Measures**

Basic Law (*Grundgesetz, GG* – extracts)

Criminal Code (*Strafgesetzbuch, StGB* – extracts)

Criminal Procedure Code (*Strafprozeßordnung, StPO* – extracts )

Act Supplementing the Act to Fight Money Laundering and Terrorist Financing (*Geldwäschebekämpfungsergänzungsgesetz, GwBekErG*)

Commercial Code (*Handelsgesetzbuch, HGB* – extracts)

Administrative Offences Act (*Ordnungswidrigkeitsgesetz, OWiG* – extracts)

Banking Act (*Kreditwesengesetz, KWG* – extracts)

Insurance Supervisory Act (*Versicherungsaufsichtsgesetz, VAG*– extracts )

Investment Act (*Investmentgesetz, InvG* – extracts)

Fiscal Code (*Abgabeordnung, AO* – extracts)

Foreign Trade and Payments Act (*Aussenwirtschaftsgesetz, AWG*– extracts )

### **1. Basic Law (Grundgesetz, GG)**

#### **Article 103 [Fair trial]**

(1) In the courts every person shall be entitled to a hearing in accordance with law.

(2) An act may be punished only if it was defined by a law as a criminal offence before the act was committed.

(3) No person may be punished for the same act more than once under the general criminal laws.

(...)

### **2. Criminal Code (Strafgesetzbuch, StGB)**

(...)

#### **Article 73 Prerequisites for Forfeiture**

(1) If an unlawful act has been committed and the perpetrator or inciter or accessory has acquired something as a result thereof or for the purpose of committing it, then the court shall order its forfeiture. This shall not apply to the extent that a claim by the aggrieved party has arisen out of the act the satisfaction of which would deprive the perpetrator or inciter or accessory of the value of that which was acquired by virtue of the act.

(2) The order of forfeiture shall extend to derived benefits. It may also extend to objects which the perpetrator or inciter or accessory has acquired through alienation of an acquired object, as a replacement for its destruction, damage or seizure or on the basis of an acquired right.

(3) If the perpetrator or inciter or accessory acted for another and the latter acquired something thereby, then the order of forfeiture under subsections (1) and (2) shall be directed at him.

(4) Forfeiture of an object shall also be ordered if it is owned or claimed by a third party, who furnished it for the act or otherwise with knowledge of the attendant circumstances of the act.

**Article 73a** Forfeiture of the Replacement Value

To the extent that the forfeiture of a particular object is impossible due to the nature of what was acquired or for some other reason or because forfeiture of a replacement object pursuant to Section 73 subsection (2), sent. 2, has not been ordered, the court shall order the forfeiture of a sum of money which corresponds to the value of that which was acquired. The court shall also make such an order collateral to the forfeiture of an object to the extent its value falls short of the value of that which was originally acquired.

(...)

**Article 73d** Extended Forfeiture

(1) If an unlawful act has been committed pursuant to a law which refers to this provision, then the court shall also order the forfeiture of objects of the perpetrator or inciter or accessory if the circumstances justify the assumption that these objects were acquired as a result of unlawful acts, or for the purpose of committing them. Sentence 1 shall also be applicable if the perpetrator or inciter or accessory does not own or have a claim to the object only because he acquired the object as a result of an unlawful act or for the purpose of committing it. Section 73 subsection (2), shall apply accordingly.

(2) If forfeiture of a particular object after the act has become impossible in whole or in part, then Sections 73a and 73b shall to that extent be applied by analogy.

(3) If, after an order of forfeiture pursuant to subsection (1) due to another unlawful act which the perpetrator or inciter or accessory committed before the order, a decision must again be made as to the forfeiture of objects of the perpetrator or inciter or accessory, then the court, in so doing, shall consider the order already issued.

(4) Section 73c shall apply accordingly.

(...)

**Section 74** Prerequisites for Confiscation

(1) If an intentional crime has been committed, then objects which were generated thereby or used or intended for use in its commission or preparation may be confiscated.

(2) Confiscation shall only be permissible if:

1. the perpetrator or inciter or accessory owns or has a claim to the objects at the time of the decision; or
2. the objects, due to their nature and the circumstances, endanger the general public or there exists a danger that they will be used for the commission of unlawful acts.

(3) Under the provisions of subsection (2), no. 2, confiscation of objects shall also be permissible if the perpetrator acted without guilt.

(4) If confiscation is prescribed or permitted by a special provision over and above subsection (1), then subsections (2) and (3) shall apply accordingly.

**Section 74a** Extended Prerequisites for Confiscation

If the law refers to this provision, then objects may also be confiscated, as an exception to Section 74 subsection (2), no. 1, if at the time of the decision the person who owns or has a claim to them:

1. has at least recklessly contributed to the fact that the property or the right thereto has been the object or instrumentality of the act or its preparation; or
2. has acquired the objects in a reprehensible manner with knowledge of the circumstances which would have permitted their confiscation.

(...)

#### **Section 74c** Confiscation of Replacement Value

(1) If the perpetrator or inciter or accessory has used, particularly through alienation or consumption, the object which he owned or had a claim to at the time of the act and which could have been subject to confiscation, or if he has otherwise obstructed the confiscation of the object, then the court may order the confiscation from the perpetrator or inciter or accessory of a sum of money no greater than an amount equivalent to the value of the object.

(2) The court may also make such an order collateral to the confiscation of an object or in place thereof, if the perpetrator or inciter or accessory has, prior to the decision on confiscation, encumbered it with the right of a third party, the extinguishment of which cannot be ordered without compensation or could not be ordered in the case of confiscation (Sections 74e subsection (2), and 74f); if the court makes the order collateral to the confiscation, then the amount of the replacement value shall be measured according to the value of the encumbrance on the object.

(3) The value of the object and the encumbrance may be estimated.

(4) In approving facilitation of payment Section 42 shall apply.

(...)

#### **Article 89a** – Preparation of a serious violent act endangering the state

(1) Whosoever prepares a serious violent act endangering the state shall be liable to imprisonment from six months to ten years. A serious violent act endangering the state is a criminal offence against life within the meaning of section 211 or section 212, or against personal freedom within the meaning of section 239a or section 239b, which under the circumstances is intended and apt to interfere with the existence or security of a state or an international organisation or to do away with, suspend the application of or undermine the constitutional principles of the Federal Republic of Germany.

(2) Subs. 1 shall apply only if the offender prepares a serious violent act endangering the state by

1. instructing another person or receiving instructions regarding the manufacture or use of firearms, explosives, explosive or incendiary devices, nuclear fuel or other radioactive substances, substances containing or capable of producing poison, other substances harmful to health, or special equipment necessary to carry out the act, or in other skills serving to commit one of the criminal offences referred to in (1) above,
2. manufacturing, procuring for himself or another, storing or making available to another weapons, substances or equipment of a type referred to in number 1 above,
3. procuring or storing items or substances crucial to the manufacture of weapons, substances or equipment of the type referred to in number 1 above,
4. collecting, accepting or making available not merely insubstantial assets for their commission.

(3) Subs. 1 shall apply equally if the preparation is undertaken in a foreign country. If the preparation is committed outside of the Member States of the European Union, this shall apply only if it is committed by a German national or a foreign national with the centre of his life inside Germany, or if the serious violent act endangering the state as prepared is to be committed inside Germany or by or against a German national.

(4) In cases of subs. 3, second sentence above, criminal prosecution shall be subject to authorisation by the Federal Ministry of Justice. If the preparation is committed in another Member

State of the European Union, criminal prosecution shall be subject to the authorisation of the Federal Ministry of Justice if such preparation is not undertaken by a German national, and the serious violent act endangering the state as prepared is not to be carried out in Germany, and is not to be committed by or against a German national.

(5) In less serious cases the penalty shall be imprisonment from three months to five years.

(6) The court may issue an order for supervision (section 68 (1); section 73d shall apply).

(7) In its discretion, the court may mitigate the sentence (section 49 (2) or order discharge pursuant to this provision if the offender voluntarily gives up the preparation of the serious violent act endangering the state, and averts or substantially reduces a danger caused and recognised by him that others will continue to prepare or carry out the act, or if he voluntarily prevents the completion of that act. If such danger is averted or substantially reduced, or if the completion of the serious violent act endangering the state is prevented regardless of the contribution of the offender, his voluntary and earnest efforts to attain that goal shall suffice.

(...)

#### **Section 129a** Formation of Terrorist Groups

(1) Whoever forms a group whose aims or activities are directed towards the commission of

1. murder (Section 211) or manslaughter (Section 212) or genocide (section 6 of the Code of Crimes against International Law) or crimes against humanity (section 7 of the Code of Crimes against International Law) or war crimes (sections 8, 9, 10, 11 or 12 of the Code of Crimes against International Law), or

2. crimes against personal liberty in the cases under Section 239a or Section 239b,

3. (deleted)

or whoever participates in such a group as a member, shall be punished by imprisonment from one year to ten years.

(2) The same punishment shall be imposable on any person who forms a group whose aims or activities are directed towards

1. causing serious physical or psychological harm to another person, especially in the way described in Section 226,

2. committing crimes under Sections 303b, 305, 305a or crimes dangerous to the general public in cases under Sections 306 to 306c or Section 307 subsections (1) to (3), Section 308 subsections (1) to (4), Section 309 subsections (1) to (5), Sections 313, 314 or Section 315 subsections (1), (3) or (4), Section 316b subsection (1) or (3) or Section 316c subsections (1) to (3) or Section 317 subsection (1),

3. committing crimes against the environment in cases under Section 330a subsections (1) to (3),

4. committing crimes under section 19 subsections (1) to (3), section 20 subsection (1) or (2), section 20a subsections (1) to (3), section 19 subsection (2), no. 2, or subsection (3), no. 2, section 20 subsection (1) or (2), or section 20a subsections (1) to (3), in each case also in conjunction with section 21, or under section 22a subsections (1) to (3) of the Act on Control of Weapons of War, or

5. committing crimes under section 51 subsections (1) to (3) of the Weapons Act;

or on any person who participates in such a group as a member, if one of the acts stipulated in nos. 1 to 5 is intended to seriously intimidate the population, to unlawfully coerce a public authority or an international organisation through the use of force or the threat of use of force, or to significantly impair or destroy the fundamental political, constitutional, economic or social structures of a country or an international organisation, and which, given the nature or consequences of such acts, may seriously damage a country or an international organisation.

(3) If the aims or activities of the group are directed towards the commission of one of the crimes referred to in subsection (1) or (2), a term of imprisonment from six months to five years shall be imposed.

(4) If the perpetrator is one of the ringleaders or persons operating behind the scenes, imprisonment for not less than three years shall be imposed in cases under subsections (1) and (2), and imprisonment from one year to ten years shall be imposed in cases under subsection (3).

(5) Whoever supports a group as described in subsection (1), (2) or (3) shall be punished by imprisonment from six months to ten years in cases under subsections (1) and (2), and by imprisonment of up to five years or a fine in cases under subsection (3) Whoever recruits members or supporters for a group as described in subsection (1) or subsection (2) shall be punished by imprisonment from six months to five years.

(6) In cases of participants whose degree of guilt is slight and whose participation is of minor significance, the court may, in cases under subsections (1), (2), (3) and (5), mitigate the severity of punishment at its discretion (Section 49 subsection (2)).

(7) Section 129 subsection (6) shall apply *mutatis mutandis*.

(8) In addition to the imposition of a term of imprisonment of at least six months, the court may also deprive the convicted person of the capacity to hold public office as well as the capacity to attain public electoral rights (Section 45 subsection (2)).

(9) In the cases under subsections (1), (2) and (4), the court may make an order for supervision of conduct (Section 68 subsection (1)).

(...)

#### **Article 261 Money Laundering; Concealment of Unlawfully Acquired Assets**

(1) Whoever hides an object which is derived from an unlawful act named in sentence 2, conceals its origin or obstructs or endangers the investigation of its origin, its being found, its forfeiture, its confiscation or its being taken into custody, shall be punished with imprisonment from three months to five years. Unlawful acts within the meaning of sentence 1 shall be:

1. serious criminal offenses;
2. less serious criminal offenses under:
  - a) Section 332 subsection (1), also in conjunction with subsection (3), and Section 334;
  - b) Section 29 subsection (1), sent. 1, no. 1, of the Narcotics Law and Section 19 subsection (1), no. 1, of the Precursors Control Law;
3. less serious criminal offenses under Section 373 and under Section 374 subsection (2) of the Fiscal Code, and also in conjunction with Section 12 subsection (1), of the Law to Implement the Common Market Organizations and Direct Payments respectively;
4. less serious criminal offenses:
  - a) under Sections 152a, 181a, 232 subsections (1) and (2), Section 233 subsections (1) and (2), Sections 233a, 242, 246, 253, 259, 263 to 264, 266, 267, 269, 284, 326 subsections (1), 2 and 4, and 328 subsections (1), 2 and 4;
  - b) under Section 96 of the Residence Act, Section 84 of the Asylum Procedure Law and under Section 374 of the Fiscal Code,

which were committed professionally or by a member of a gang which has combined for the continued commission of such acts; and

5. less serious criminal offences under sections 129 and 129a subsections (3) and (5), each of which also in conjunction with section 129b subsection (1), as well as less serious offences

committed by a member of a criminal or terrorist organisation (sections 129 and 129a, each of which also in conjunction with section 129b subsection (1)).

Sentence 1 shall apply, in cases of tax evasion committed on a commercial or gang basis under Section 370a of the Fiscal Code, to expenditure saved by virtue of the tax evasion, of unlawfully acquired tax repayments and allowances, and in cases under sentence 2, number 3, sentence 1 shall also apply to an object in relation to which fiscal charges have been evaded.

(2) Whoever:

1. procures an object indicated in subsection (1) for himself or a third person; or
2. keeps an object indicated in subsection (1) in his custody or uses it for himself or a third person,

shall be similarly punished.

(3) An attempt shall be punishable.

(4) In especially serious cases the punishment shall be imprisonment from six months to ten years. An especially serious case exists, as a rule, if the perpetrator acts professionally or as a member of a gang, which has combined for the continued commission of money laundering.

(5) Whoever, in cases under subsections (1) or (2), is recklessly unaware, that the object is derived from an unlawful act named in subsection (1), shall be punished with imprisonment for not more than two years or a fine.

(6) The act shall not be punishable under subsection (2), if a third person previously acquired the object without having thereby committed a crime.

(7) Objects to which the crime relates may be confiscated. Section 74a shall be applicable. Sections 43a, 73d shall be applicable if the perpetrator acts as a member of a gang which has combined for the continued commission of money laundering. Section 73d shall also be applicable if the perpetrator acts professionally.

(8) Objects which are derived from an act of the type indicated in subsection (1) committed overseas shall be the equivalent of the objects indicated in subsections (1), (2), and (5), if the act is also punishable at the place of commission of the act.

(9) Whoever:

1. voluntarily reports the act to the competent public authority or voluntarily causes such a report to be made, if the act was not already discovered in whole or in part at the time and the perpetrator knew this or should have taken this into account upon a reasonable evaluation of the factual situation; and
2. in cases under subsections (1) or (2) under the prerequisites named in number 1, causes the object to which the crime relates to be taken into custody,

shall not be punished under subsections (1) to (5).

Whoever is punishable because of participation in the antecedent act shall also not be punished under subsections (1) to (5).

(10) The court in its discretion may mitigate the punishment (Section 49 subsection (2)) in cases under subsections (1) to (5) or dispense with punishment under these provisions, if the perpetrator through voluntary disclosure of his knowledge has substantially contributed, so that the act, beyond his own contribution thereto, or an unlawful act of another named in subsection (1), could be uncovered.

(...)

### **3. Criminal Procedure Code (Strafprozeßordnung, StPO)**

(...)

#### **Article 111b. [Securing of Objects]**

(1) Objects may be secured by seizure pursuant to Section 111c if there are grounds to assume that the conditions for their forfeiture or for their confiscation have been fulfilled. Section 94 subsection (3) shall remain unaffected.



(2) If there are grounds to assume that the conditions have been fulfilled for forfeiture of [the pecuniary] equivalent [of the ]value or for confiscation of the pecuniary equivalent of the value of the object, attachment *in rem* may be ordered pursuant to Section 111d in order to secure such equivalent value.

(3) If there are no cogent grounds, the court may revoke the order in respect of the measures referred to in the first sentence of subsection (1) and in subsection (2) after a maximum period of six months. Where certain facts substantiate the suspicion [of the offence] and the time limit referred to in the first sentence is not sufficient given the particular difficulty or particular extent of the investigations or for another important reason, the court may, upon application by the public prosecution office, extend the measure provided the grounds referred to justify their continuation. Unless there are cogent grounds, the measure shall not be continued for longer than a period of twelve months.

(4) Sections 102 to 110 shall apply *mutatis mutandis*.

(5) Subsections (1) to (4) shall apply *mutatis mutandis* insofar as forfeiture may not be ordered for the sole reason that the conditions under section 73 subsection (1), second sentence, of the Criminal Code apply.

#### **Article 111c. [Securing Seizure]**

(1) Seizure of a moveable asset shall be effected in the cases referred to under Section 111b by impounding the asset or by indicating the seizure by seal or in some other way.

(2) Seizure of a plot of land or of a right subject to the provisions on compulsory execution in respect of immovable property shall be effected by making an entry concerning the seizure in the Land Register. The provisions of the Act on Compulsory Sale by Public Auction and Compulsory Administration in respect of the extent of seizure on compulsory sale by public auction shall apply *mutatis mutandis*.

(3) Seizure of a claim or any other property right not subject to the provisions on compulsory execution in respect of immovable property shall be effected by attachment. The provisions of the Civil Procedure Code on compulsory execution in respect of claims and other property rights shall apply *mutatis mutandis*. The request to make the declarations referred to in section 840 subsection (1) of the Civil Procedure Code shall be linked to seizure.

(4) Seizure of ships, ship constructions and aircraft shall be effected pursuant to subsection (1). The seizure shall be entered in the Register in respect of those ships, ship constructions and aircraft that are entered in the Register of Ships, in the Register of Ship Constructions or in the Register of Liens on Aircraft. Application for such entry may be made in respect of ship constructions or aircraft that have not been, but are capable of being, entered in the Register; the provisions governing an application by a person who is entitled to request entry in the Register by virtue of an executory title shall apply *mutatis mutandis* in this case.

(5) Seizure of an object pursuant to subsections (1) to (4) shall have the effect of a prohibition of alienation within the meaning of section 136 of the Civil Code; the prohibition shall also cover other directions besides alienation.

(6) A moveable asset that has been seized may:

1. be handed over to the person concerned against immediate payment of its value or
2. be retained by the person concerned, subject to revocation at any time, for further use in the interim until conclusion of the proceedings.

The sum paid pursuant to the first sentence, number 1, shall be substituted for the asset. The measure pursuant to the first sentence, number 2, may be made dependent on the person concerned providing security or fulfilling certain conditions.

#### **Article 111d. [Attachment for Equivalent Value; Fine or Costs]**

(1) Attachment *in rem* may be ordered by virtue of forfeiture or of confiscation of equivalent value, by virtue of a fine or of the anticipated costs of criminal proceedings. Attachment may only be ordered by virtue of a fine or of the anticipated costs if judgment has been passed against the defendant imposing punishment. Attachment shall not be ordered to secure execution costs or negligible amounts.

(2) Sections 917 and 920 subsection (1) as well as sections 923, 928, 930 to 932, and 934 subsection (1) of the Civil Procedure Code shall apply *mutatis mutandis*.

(3) If attachment has been ordered by virtue of a fine or of the anticipated costs, an enforcement measure shall be revoked upon application by the defendant if the defendant needs the object of attachment to pay the costs of his defence, his maintenance or the maintenance of his family.

**Article 111e.** [Order for Seizure or Attachment]

(1) Only the court, and in exigent circumstances also the public prosecution office, shall be competent to order seizure (Section 111c) and attachment (Section 111d). Officials assisting the public prosecution office (section 152 Courts Constitution Act) shall also be competent to order seizure of a moveable asset (Section 111c, subsection (1)) in exigent circumstances.

(2) If the public prosecution office has ordered seizure or attachment, it shall apply for judicial confirmation of the order within one week. This shall not apply when seizure of a moveable asset has been ordered. In all cases the person concerned may apply for a judicial decision at any time.

(3) The public prosecution office shall inform the person who is aggrieved as a result of the act without delay of enforcement of the order for seizure or attachment, insofar as his identity is known or becomes known during the course of proceedings.

(4) If notifying each aggrieved person individually would result in a disproportionate amount of effort or if it may be assumed that other yet unknown aggrieved persons have claims arising from the act, notice may be given of the seizure or attachment by insertion once in the electronic Federal Gazette. In addition notice may also be published in some other suitable manner. Personal data may only be published insofar as its provision is essential in order to enable the aggrieved persons to access the secured assets in order to enforce their claims. Once the security measures have been concluded the public prosecution office shall initiate the deletion of the publication inserted in the electronic Federal Gazette.

**Article 111f.** [Effecting Seizure and Enforcing Attachment]

(1) Effecting seizure (Section 111 c) shall be incumbent upon the public prosecution office and, in the case of moveable assets (Section 111 c subsection (1)), also upon the officials assisting it. Section 98 subsection (4) shall apply *mutatis mutandis*.

(2) The required entries in the Land Register as well as in the registers referred to in Section 111c subsection (4) shall be made upon application by the public prosecution office or by the court that ordered seizure. The same shall apply *mutatis mutandis* to the applications referred to in Section 111c subsection (4).

(3) If enforcement of attachment is to be effected pursuant to the provisions on attachment of moveable assets, this may be effected by the authority designated in section 2 of the Ordinance on Recovery of Claims of the Judicial Authorities, by the court bailiff, the public prosecution office, or the officials assisting it (section 152 of the Courts Constitution Act). Subsection (2) shall apply *mutatis mutandis*. The public prosecution office or, upon the application of the public prosecution office, the court that ordered the attachment shall be competent to order attachment of a registered ship or ship construction and to order attachment of a claim arising out of the attachment pursuant to Section 111d.

(4) Section 37 subsection (1) shall apply to service, subject to the proviso that the officials assisting the public prosecution office (section 152 of the Courts Constitution Act) may also be assigned the task of enforcing the order.

(5) The person concerned may at any time apply for a judicial decision in respect of measures taken in the course of enforcing the seizure or attachment.

**Article 111g. [Compulsory Execution; Enforcement of Attachment by the Aggrieved Person]**

(1) Seizure of an object pursuant to Section 111c and the enforcement of attachment pursuant to Section 111d shall not take effect against a disposition made by the aggrieved person, by way of compulsory execution or enforcement of attachment on the basis of a claim arising from the criminal offence.

(2) Compulsory execution or enforcement of attachment pursuant to subsection (1) shall require the approval of the court which is competent to order seizure (Section 111c) or attachment (Section 111d). The decision shall be given in the form of an order that may be contested by the public prosecution office, the accused and the aggrieved person by means of an immediate complaint. Approval shall be refused if the aggrieved person cannot furnish prima facie evidence that the claim arose from the criminal offence. Section 294 of the Civil Procedure Code shall apply.

(3) The prohibition of alienation pursuant to Section 111c subsection (5) shall apply from the moment of seizure also for the benefit of aggrieved persons who, during seizure, pursue compulsory execution in respect of the object seized or who enforce attachment. Entry of the prohibition of alienation in the Land Register for the benefit of the state shall also apply, for the purposes of section 892 subsection (1), second sentence, of the Civil Code, as an entry for the benefit of those aggrieved persons who, during seizure, are entered in the Land Register as beneficiaries of the prohibition of alienation. Proof that the claim arose from the criminal offence can be furnished to the Land Registry by submission of the order granting approval. The second and third sentences shall apply *mutatis mutandis* to the prohibition of alienation in the case of ships, ship constructions and aircraft referred to in Section 111c subsection (4). The legal force of the prohibition of alienation for the benefit of the aggrieved person shall not be affected by revocation of seizure. The first and fifth sentences shall apply *mutatis mutandis* for the effect of the lien which arises in respect of the moveable assets through the enforcement of the attachment (Section 111d).

(4) If the object seized or attached on the grounds of attachment is not subject to forfeiture on grounds other than those referred to in section 73 subsection (1), second sentence, of the Criminal Code, or if approval was wrongfully granted, the aggrieved person shall be obliged to compensate third parties for the damage caused to them due to the fact that the prohibition of alienation applies for his benefit pursuant to subsection (3).

(5) Subsections (1) to (4) shall apply *mutatis mutandis* if forfeiture of an object has been ordered but the order has not yet become binding. They shall not apply if the object is subject to confiscation.

**Article 111h. [Prior Satisfaction of Claims of the Aggrieved Person on Attachment]**

(1) If the aggrieved person applies for compulsory execution in respect of a claim arising from the criminal offence or if he enforces attachment in respect of a plot of land where attachment has been enforced pursuant to Section 111d, he may demand that his right shall have priority over the collateral mortgage established by enforcement of that attachment. The priority of such right shall not be lost by virtue of revocation of the attachment. The consent of the owner shall not be required for the change of priority. In all other respects section 880 of the Civil Code shall be applied accordingly.

(2) The change of priority shall require approval by the judge who is competent to order attachment (Section 111d). Section 111 g subsection (2), second to fourth sentences, and subsection (3), third sentence, shall apply *mutatis mutandis*.

(3) If approval was wrongfully granted, the aggrieved person shall be obliged to compensate third persons for the damage caused to them due to the change of priority.

(4) Subsections (1) to (3) shall apply *mutatis mutandis* if attachment pursuant to Section 111d is enforced in respect of a ship, a ship construction or an aircraft as defined in Section 111c subsection (4), second sentence.

**Article 111i. [Maintenance of Seizure]**

(1) The court may order that seizure pursuant to Section 111c or attachment pursuant to Section 111d be maintained for a maximum period of three months, as long as the proceedings pursuant to Sections 430 and 442, subsection (1) are confined to the other legal consequences and the immediate revocation would be unjust in respect of the aggrieved person.

(2) If the court did not order forfeiture simply because claims of an aggrieved person within the meaning of section 73 subsection (1), second sentence of the Criminal Code present an obstacle to this, it may state this in the judgment. In such a case, it has to describe that which was acquired. Insofar as the preconditions for section 73a of the Criminal Code apply, the court shall determine a sum of money equivalent to the value of that which was acquired. Insofar as

1. the aggrieved person has already taken action by way of compulsory execution or enforcement of attachment,
2. it is proven that the aggrieved person was satisfied out of assets that were not seized or pledged by way of enforcement of attachment, or
3. that which was acquired was delivered to the aggrieved person pursuant to Section 111k,

this is to be deducted as part of the assessment to be made pursuant to the second and third sentences.

(3) Insofar as the court proceeds pursuant to Subsection (2), it shall maintain the seizure (Section 111c) of that which was acquired as defined in subsection (2), second and fourth sentences, as well as the attachment *in rem* (Section 111d) up to the amount of the sum determined pursuant to subsection (2), third and fourth sentences, for three years in its order. Time shall start to run with effect from the binding judgment. Secured assets shall be listed in the order. Section 917 of the Civil Procedure Code shall not apply. If it is proven that the aggrieved person was satisfied out of assets that were not seized or attached by way of enforcement of attachment, the court shall revoke the seizure (Section 111c) or attachment *in rem* (Section 111d) upon application by the person concerned.

(4) The court shall notify the person aggrieved by the act without delay of the order made pursuant to subsection (3) as well as the fact of its entry into force. With the notification, attention is to be drawn to the consequences listed in subsection (5) and to the option of enforcing claims by way of compulsory execution or enforcement of attachment. Section 111e subsection (4), first to third sentences shall apply *mutatis mutandis*.

(5) Upon expiry of the time limit specified in subsection (3) the state shall acquire the assets listed in accordance with subsection (2) pursuant to section 73e subsection (1) of the Criminal Code, as well as a right to payment in the amount of the sum assessed pursuant to subsection (2), unless

1. the aggrieved person has in the mean time already taken action by way of compulsory execution or enforcement of attachment in respect of his claim,
2. it is proven that the aggrieved person was satisfied out of assets that were not seized or attached by way of enforcement of attachment, or
3. objects have in the meantime been delivered to the aggrieved person or deposited pursuant to Section 111k, or
4. the aggrieved person would have been entitled to objects pursuant to Section 111k and he applied for their delivery prior to expiry of the time limit specified in subsection (3).

At the same time, the state may realize the lien based on enforcement of attachment *in rem* in accordance with the provision of Part Eight of the Civil Procedure Code. The proceeds as well as any money deposited as security shall fall to the state. Upon realization the right to payment which arose

pursuant to the first sentence also expires insofar as the proceeds of realization do not exceed the amount of the claim.

(6) The court of first instance shall issue an order confirming the occurrence, and extent, of the acquisition of rights by the state pursuant to subsection (5) first sentence. Section 111 l subsection (4) shall apply *mutatis mutandis*. The order may be challenged by way of immediate complaint. Once the order has legal force the court shall initiate the deletion of the publications in the electronic Federal Gazette initiated pursuant to subsection (4).

(7) Insofar as the person convicted or affected by the seizure or attachment in rem satisfies the claims of the aggrieved person secured thereby after expiry of the time limit specified in subsection (3), he may demand compensation up to the amount received by the state for the realization. The right to compensation shall be excluded

1. insofar as the state's right to payment pursuant to subsection (5), first sentence, taking into account the proceeds received by the state, precludes it or

2. if three years have passed since expiry of the time limit set out in subsection (3).

(8) In the cases referred to in section 76a subsection (1) or 3 of the Criminal Code, subsections (2) to (7) are to be applied *mutatis mutandis* to the proceedings pursuant to Sections 440 and 441 in conjunction with Section 442 subsection (1).

#### **Article 111k. [Return of Moveable Assets to the Aggrieved Person]**

Moveable assets which have been seized or otherwise secured pursuant to Section 94 or which have been seized pursuant to Section 111c subsection (1) should be handed over to the aggrieved person, from whom they have been taken as a result of the criminal offence if his identity is known, if the claims of third persons do not present an obstacle and if the assets are no longer required for the purposes of the criminal proceedings. The public prosecution office can obtain a judicial decision if the rights of the aggrieved person are not evident.

#### **Article 111l. [Emergency Sale]**

(1) Objects which have been seized pursuant to Section 111c, as well as objects which have been attached (Section 111d), may be sold before the judgment becomes final if they are subject to deterioration or substantial reduction of their value, or if their preservation, care or maintenance would result in disproportionately high costs or difficulties. In the cases set out in Section 111i subsection (2) assets which have been attached (Section 111d) may be sold after the judgment has become binding, if this appears expedient. The proceeds shall be substituted for the objects.

(2) The emergency sale shall be ordered by the public prosecution office in the preparatory proceedings and after the judgment has become final. The officials assisting it (section 152 of the Courts Constitution Act) shall have the authority to order such sale if there is a danger that the object will be subject to deterioration before the decision of the public prosecution office can be obtained.

(3) Upon preferring public charges the order shall be made by the court seized of the main proceedings. The public prosecution office shall have the authority to make such order if the object is subject to deterioration before the decision of the court can be obtained; subsection (2), second sentence, shall apply *mutatis mutandis*.

(4) The accused, the owner and other persons who have rights in relation to the object shall be heard prior to the order. The order, as well as time and place of the sale, shall be made known to them as far as this appears to be practicable.

(5) The emergency sale shall be carried out in accordance with the provisions of the Civil Procedure Code concerning the use/realization of an attached object. The public prosecution office shall take the place of the court responsible for execution (section 764 of the Civil Procedure Code) in the cases referred to in



subsections (2) and (3), second sentence; in the case of subsection (3), first sentence, the court seized of the main proceedings. The realization admissible pursuant to section 825 of the Civil Procedure Code may be ordered at the same time as the emergency sale or subsequently, either *proprio motu* or upon application of the persons designated in subsection (4), or in the case of subsection (3), first sentence, also upon application by the public prosecution office. If it appears expedient, an emergency sale may be ordered in some other manner and by a person other than the bailiff.

(6) The person concerned may request a court decision regarding orders of the public prosecution office or the officials assisting it. Section 161a subsection (3), second to fourth sentence, shall apply *mutatis mutandis* with the proviso that after public charges have been preferred the court seized of the main proceedings shall be competent to decide and once the judgment has entered into force the court of first instance shall be competent to decide. The court, and in urgent cases the presiding judge, may order suspension of the sale.

(...)

#### **4. Act Supplementing the Act to Fight Money Laundering and Terrorist Financing (Geldwäschebekämpfungsergänzungsgesetz, GwBekErG)**

*Unofficial translation of the Act to enhance the fight against money laundering and financing of terrorism as published on the 20<sup>th</sup> of August 2008 (Federal Law Gazette I, p. 1690) which entered in to force on the 21<sup>st</sup> of August 2008*

#### **Act by the Federal Government of the 13<sup>th</sup> of August 2008**

#### **Act to enhance the fight against money laundering and financing of terrorism (Act Supplementing the Act to Fight Money Laundering and Terrorist Financing (GwBekErgG))**

##### **A. Problem and objective**

Directive 2005/60/EC of the European Parliament and the Council<sup>83</sup> and Directive 2006/70/EC<sup>84</sup> of the Commission reorganized and expanded the foundations for national legislation to fight money laundering and terrorist financing. The objective of this Act is to implement the substance of these two Directives in national law.

##### **B. Solution**

Overhauling the Money Laundering Act and amending the Banking Act and Act on the Supervision of the Insurance Industry has extended instruments developed to fight money laundering also to terrorist financing, has refined the requirements of due diligence on the part of obligated institutions and persons in line with the principle of risk orientation, and introduced the requirement to identify the beneficial owner behind the contracting party.

In addition, the definition of money laundering crime was revised in the Criminal Code; as a result, amendments were made to the Customs Administration Act, the Investment Act, the Ordinance on the imposition of fees and the allocation of costs pursuant to the Act on Financial Services Supervision, the

<sup>83</sup> Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

<sup>84</sup> Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of politically exposed persons and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis.



Ordinance on monthly financial statements and the Ordinance on auditor's reports; and the Act on Financial Services Supervision was revised with regard to fee regulations.

### **C. Alternatives**

None.

### **D. Financial impact on public budgets**

No impacts on public budget revenues or expenditures are anticipated.

### **E. Other costs**

The new information and record-keeping obligations will cause minor additional costs to private business, which are likely to have a minor impact on individual prices. There are no other costs to the private sector. No additional impacts of the legislation for individual prices, the overall price level or consumer prices can be expected.

### **F. Administrative costs**

The Act includes six new reporting requirements for the private sector. Six existing reporting requirements for the private sector will be revised. An ex ante assessment indicates that increased costs of about EUR 195 000 can be expected.

The Act includes a new reporting requirement for individuals.

Four reporting requirements for public administration were revised.

### **Act to enhance the fight against money laundering and financing of terrorism (Act Supplementing the Act to Fight Money Laundering and Terrorist Financing (GwBekErgG))<sup>85</sup>**

The Bundestag has adopted the following Act with the approval of the Bundesrat:

#### **Article 1**

#### **Amendment of the Criminal Code**

Section 261 of the Criminal Code as published on 13 November 1998 (Federal Law Gazette I, p. 3322), last amended by Article ... of the Act of (Federal Law Gazette I, p. ), shall be amended as follows:

1. (1) second sentence no. 4 ad a shall be amended as follows:
  - a) The figure "271" shall be inserted after the figure "269".
  - b) The phrase "as well as" shall be replaced by a comma.

---

<sup>85</sup>

This Act implements the following Directives:

- Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJ L 309 p. 15), last amended by Directive 2007/64/EC of the European Parliament and the Council of 13 November 2007 (OJ L 319 p. 1);

- Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of politically exposed persons and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis (OJ L 214 p. 29).

- c) The text “as well as Section 348” shall be inserted after the text “Section 328 (1), (2) and (4)”.
2. Paragraph 7 third and fourth sentences shall be replaced by the following sentence:
- “Section 73d shall be applied to any perpetrator acting on a commercial basis or as a member of a gang formed for the purpose of repeatedly committing such offences.”

**Article 2**

**Act on the Detection of Proceeds from Serious Crimes (Money Laundering Act (GwG))**

## Table of Contents

### Chapter 1 Definitions and scope

Section 1	Definitions
Section 2	Scope

### Chapter 2 Due diligence and internal safeguards

Section 3	General provisions
Section 4	Identification
Section 5	Simplified due diligence
Section 6	Enhanced due diligence
Section 7	Performance by third parties
Section 8	Record-keeping
Section 9	Internal safeguards

### Chapter 3 Financial Intelligence Unit, reporting requirements and use of data

Section 10	Financial Intelligence Unit
Section 11	Suspicious transaction reports
Section 12	Prohibition of transmission of information
Section 13	Release from responsibility
Section 14	Suspicious transaction reports filed by government authorities
Section 15	Reference to and use of records

### Chapter 4 Supervision and administrative fines

Section 16	Supervision
Section 17	Administrative fines

## Chapter 1 Definitions and scope

### Section 1 Definitions

- (1) For the purposes of this Act, “identification” means
1. establishing identity by gathering information and
  2. verifying identity.
- (2) For the purposes of this Act, “terrorist financing” means the provision or collection of funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, to carry out the following:
1. an offence within the meaning of Section 129a, also in conjunction with Section 129b of the Criminal Code, or
  2. any of the offences within the meaning of Articles 1 to 3 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, p. 3)
- or to aid or facilitate the commission of such activity.
- (3) For the purposes of this Act, “business relationship” means a business or professional relationship which is directly connected with the professional activities of the institutions and persons covered by this Act and which is expected, at the time when the contact is established, to have an element of duration.
- (4) For the purposes of this Act, “transaction” means any act aimed at or resulting in a transfer of money or a similar movement of assets.
- (5) For the purposes of this Act, electronic cash as defined in Section 1 (14) of the Banking Act shall be the equivalent of cash.
- (6) For the purposes of this Act, “beneficial owner” means the natural person(s) who ultimately owns or controls the contracting party, or the natural person on whose behalf a transaction or activity is being conducted. This includes in particular:
1. in the case of corporate entities which are not listed on a regulated market as defined in Section 2 (5) of the Securities Trading Act and are not subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards: the natural person(s) who directly or indirectly hold more than 25% of the capital shares or control more than 25% of the voting rights;
  2. in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds or arrange for third parties to administer and distribute funds:
    - a) the natural person(s) who exercises control over 25% or more of the property of a legal arrangement or entity;
    - b) the natural person(s) who is the beneficiary of 25% or more of the property of a legal arrangement or entity;
    - c) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates.
- (7) In consultation with the Federal Ministry of Finance and the Federal Ministry of Economics and Technology, the Federal Ministry of the Interior may, by means of statutory instruments without the approval of the Bundesrat and in compliance with the implementation measures taken by the Commission

of the European Union based on Article 40 (1) a of Directive 2005/60/EC of the European Parliament and the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJ L 309, p. 15), specify the previous definitions in further detail.

## Section 2

### Scope

(1) This Act shall apply to the following acting in the exercise of their business or professional activities:

1. credit institutions as defined in Section 1 (1) of the Banking Act (with the exception of those institutions listed in Section 2 (1) nos. 3 to 8 of the Banking Act) and domestic branches of credit institutions having their head offices abroad;
2. financial services institutions as defined in Section 1 (1a) of the Banking Act (with the exception of those institutions listed in Section 2 (6) nos. 3 to 12 and (10) of the Banking Act) and domestic branches of financial services institutions having their head offices abroad;
3. financial enterprises as defined in Section 1 (3) of the Banking Act which do not come under 1. or 4. and whose main activity is the equivalent of one of the main activities listed in Section 1 (3) first sentence of the Banking Act or of a main activity of an enterprise designated by statutory instrument under Section 1 (3) second sentence of the Banking Act, and the domestic branches of such enterprises having their head offices abroad;
4. insurance companies conducting business covered by Directive 2002/83/EC of the European Parliament and the Council of 5 November 2002 concerning life assurance (OJ L 345, p. 1) or providing accident insurance with premium redemption, and the domestic branches of such companies having their head offices abroad;
5. insurance intermediaries as defined in Section 59 of the Insurance Contract Act when they act in respect of life insurance and other investment-related services (with the exception of insurance intermediaries operating in accordance with Section 34d (3) or (4) of the Trade Regulations Act), and domestic branches of such insurance intermediaries having their head offices abroad;
6. investment companies as defined in Section 2 (5) of the Investment Act and investment management companies as defined in Section 2 (6) of the Investment Act and domestic branches of such companies having their head offices abroad;
7. Lawyers, legal advisers who are members of a chamber of lawyers and registered persons as defined in Section 10 of the Legal Services Act, patent lawyers and notaries when they assist in the planning or execution of the following transactions for their clients:
  - a) buying and selling of real property or business entities,
  - b) managing of client money, securities or other assets,
  - c) opening or management of bank, savings or securities accounts,
  - d) procurement of funds required for the creation, operation or management of companies,
  - e) creation, operation or management of trusts, companies or similar structures,or when they act on behalf of and for their client in any financial or real estate transaction.
8. auditors, chartered accountants, tax advisers and tax agents;
9. trust or company service providers not already covered under 7. or 8. when they provide the following services for third parties:
  - a) creating a legal person or partnership;
  - b) acting as a director or manager of a legal person or partnership, a partner of a partnership or a similar position;
  - c) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement as defined in Section 1 (6) second sentence no. 2;
  - d) acting as a trustee of a legal arrangement as defined in Section 1 (6) second sentence no. 2;

- e) acting as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements as defined in Section 2 (5) of the Securities Trading Act in conformity with Community legislation or subject to equivalent international standards;
- f) arranging for another person to act in the functions described under b, d and e;
- 10. real estate agents;
- 11. gambling casinos;
- 12. persons trading in goods.

(2) In compliance with the implementation measures taken by the Commission of the European Union under Article 40 (1) d of Directive 2005/60/EC and within the framework of their jurisdiction for legal and natural persons as defined in (1) nos. 1 to 6, the federal ministries of the Interior, Finance, and Economics and Technology may, by means of statutory instruments, without the approval of the Bundesrat, exempt legal and natural persons from legal requirements intended to prevent money laundering or terrorist financing, where such persons engage in a financial activity on an occasional or very limited basis and where there is little risk of money laundering or terrorist financing occurring. The Federal Ministry of Finance may, by means of statutory instruments without the approval of the Bundesrat, delegate its authority to the Federal Financial Supervisory Authority (BAFin).

## Chapter 2 Due diligence and internal safeguards

### Section 3 General provisions

- (1) The institutions and persons defined in Section 2 (1) shall, in the cases listed in paragraph 2, carry out the following general due diligence measures:
1. verify the identity of the contracting party as described in Section 4 (3) and (4);
  2. obtain information on the purpose and intended nature of the business relationship if the business relationship does not already make them clear beyond doubt;
  3. clarify whether the contracting party is acting on behalf of a beneficial owner and if so, identify the beneficial owner as described in Section 4 (5); if the contracting party is not a natural person, this includes the duty to take adequate measures to understand the ownership and control structure of the contracting party;
  4. continuously monitor the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the contracting party and beneficial owner, if applicable, the business and risk profile, including, where necessary, the source of funds and ensure that the documents, data or information are updated at appropriate intervals.
- (2) Due diligence as described in paragraph 1 shall be applied
1. when establishing a business relationship;
  2. when carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations totalling EUR 15 000 or more which appear to be linked;
  3. when there is reason to suspect that a transaction may have served or would serve the purpose of an offence pursuant to Section 261 of the Criminal Code or of terrorist financing, regardless of any derogation, exemption or threshold;
  4. when there are doubts about the veracity or adequacy of data identifying the contracting party or beneficial owner gathered on the basis of this Act.



The first sentence, no. 1 shall not apply to institutions or persons as defined in Section 2 (1) no. 12. The first sentence, no. 2 shall apply to institutions or persons as defined in Section 2 (1) no. 12 only when accepting cash amounting to EUR 15 000 or more.

(3) Without prejudice to paragraph 2, institutions and persons as defined in Section 2 (1) no. 11 shall be required to verify the identity of customers buying or exchanging gambling chips with a value of EUR 2 000 or more. This requirement may also be met by verifying the identity of customers when they enter the gambling casino.

(4) The institutions and persons covered by this Act shall apply each of the customer due diligence measures set out in paragraph 1, but may determine the extent of such measures on a risk-sensitive basis depending on the type of contracting party, business relationship, product or transaction. The institutions and persons covered by this Act shall be able to demonstrate to the competent authorities mentioned in Section 16 (2) that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

(5) Insurance intermediaries as defined in Section 2 (1) no. 5 who collect premiums for an insurance company as defined in Section 2 (1) no. 4, shall inform the insurance company when premiums are paid in cash and amount to more than EUR 15 000 within a calendar year.

(6) If an institution or person covered by this Act is unable to fulfil the requirements of due diligence laid down in paragraph 1 nos. 1 to 3, then it may not establish or continue the business relationship or carry out any transactions. If a business relationship already exists, the institution or person covered by this Act shall terminate this relationship regardless of other legal or contractual provisions. Sentences 1 and 2 do not apply to institutions or persons as defined in Section 2 (1) nos. 7 and 8 when the contracting party seeks legal advising or representation in proceedings unless the institution or person concerned knows that the contracting party is utilizing the legal advice for the purpose of money laundering or terrorist financing.

## Section 4

### Identification

(1) Institutions and persons covered by this Act shall identify the contracting parties and beneficial owners, if applicable, before establishing a business relationship or carrying out a transaction. Identification may be completed while the business relationship is being established if this is necessary to avoid interrupting the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring.

(2) If institutions and persons covered by this Act have already identified the relevant contracting parties and beneficial owners and made a record of the information gathered, they do not need to repeat such identification unless external circumstances lead them to doubt whether the information gathered previously to identify the persons in question is still valid.

(3) To establish the identity of the contracting party, institutions and persons covered by this act shall gather the following information:

1. for natural persons: name, place and date of birth, nationality and address;
2. for legal persons or partnerships: company, name or title, legal form, registry number if available, address of headquarters or head office, names of members of the representative body or legal representatives; if a member of the representative body or legal representation is a legal person, the following information of this legal person shall be gathered: company, name or title, legal form, registry number if available and address of headquarters or main office.

(4) To verify the contracting party's identity, institutions and persons covered by this Act shall check the accuracy of the information gathered pursuant to paragraph 3 and contained in the following documents by using these documents, also if they do not contain all of the information:

1. for natural persons, save as provided in Section 6 (2) no. 2: valid official identity card including the holder's photograph which satisfies domestic requirements for identity cards or passports, in particular domestic passports and passports, identity cards or their substitutes recognized or accepted under foreigners law;
2. for legal persons or partnerships: a copy of the relevant entry in the commercial register or register of cooperative societies or similar official register; foundation charters or equivalent documents; or access to the register data.

In consultation with the Federal Ministry of Finance, the Federal Ministry of the Interior may, by means of statutory instruments without the approval of the Bundesrat, designate additional documents suitable for verifying identity.

(5) In the case of beneficial owners, institutions and persons covered by this Act shall find out at least the name of the beneficial owner and gather further identification depending on the level of risk of money laundering or terrorist financing in the individual case. To verify the beneficial owner's identity, institutions and persons covered by this Act shall take risk-adequate measures to check the accuracy of the information gathered pursuant to the first sentence.

(6) The contracting party shall provide the necessary information and documents for the institutions and persons covered by this Act to meet due diligence requirements and shall inform them of any changes without delay as long as they maintain a business relationship.

## Section 5

### Simplified due diligence

(1) If the conditions for Section 6 are not met, in the cases of Section 3 (2) first sentence nos. 1, 2 and 4 the institutions and persons covered by this Act may be exempted from the due diligence requirements listed in Section 3 (1) if there is a low risk of money laundering or terrorist financing as defined in paragraph 2. Section 3 (4) second sentence shall apply *mutatis mutandis*.

(2) Unless otherwise indicated in Section 25d of the Banking Act, also in conjunction with Section 6 (5) of the Investment Act and Section 80e of the Act on the Supervision of the Insurance Industry, only the following qualify as low-risk cases:

1. transactions by or on behalf of, or when establishing business relationships with, institutions or persons as defined in Section 2 (1) nos. 1 through 6; the same applies to credit or financial institutions as defined in Directive 2005/60/EC which have a main office in a European Union Member State or in third countries provided that they are subject to equivalent requirements and are supervised for compliance with those requirements;
2. transactions by or on behalf of, or when establishing business relationships with, listed companies whose securities are admitted to trading on a regulated market as defined in Section 2 (5) of the Securities Trading Act in one or more European Union Member States and listed companies from third countries which are subject to disclosure requirements consistent with Community legislation;
3. when identifying the beneficial owner of third-party accounts of institutions and persons as defined in Section 2 (1) no. 7, if the information on the identity of the beneficial owner is available, on request, to the institutions that act as depository institutions for the accounts; the same applies to accounts held by notaries and other independent legal professionals from the European Union Member States, or from third countries provided that they are subject to

requirements to combat money laundering or terrorist financing consistent with international standards and are supervised for compliance with those requirements;

4. transactions by or on behalf of, or when establishing business relationships with, domestic public authorities as defined in Section 1 (4) of the Administrative Procedures Act and the corresponding provisions of the administrative procedures legislation of the states (*Länder*); the same shall apply to foreign public authorities or institutions entrusted with public functions pursuant to the Treaty on European Union, the Treaties on the Communities or Community secondary legislation, provided that their identity is publicly available, transparent and certain, their activities and accounting practices are transparent and they are accountable to a Community institution or to the authorities of a Member State or other measures of supervision and oversight.

Section 25d of the Banking Act shall apply *mutatis mutandis* to institutions and persons as defined in Section 2 (1) no. 3.

(3) Paragraphs 1 and 2 shall not apply when the institutions or persons covered by this Act have information about a specific transaction or business relationship indicating a higher risk of money laundering or terrorist financing.

(4) In consultation with the Federal Ministry of Finance and the Federal Ministry of Economics and Technology, the Federal Ministry of the Interior may, by means of statutory instruments without the approval of the Bundesrat

1. define additional criteria for a low risk of money laundering or terrorist financing in order to implement measures taken by the European Commission in accordance with Article 40 (1) b of Directive 2005/60/EC;
2. implement a decision of the European Commission in accordance with Article 40 (4) of Directive 2005/60/EC with regard to the cases described in Article 12 of this Directive.

## Section 6

### Enhanced due diligence

(1) In situations where higher risk of money laundering or terrorist financing could apply, the institutions and persons covered by this Act shall apply enhanced due diligence measures appropriate to the higher risk. Section 3 (4) second sentence and (6) shall apply *mutatis mutandis*.

(2) In the following higher-risk cases in particular, the following enhanced due diligence measures shall be carried out:

1. Institutions and persons covered by this Act shall take appropriate risk-based measures to determine whether the contracting party is a natural person based outside the country who is or has been entrusted with prominent public functions, or immediate family members or persons known to be close associates to such a person as defined in Article 2 of Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of politically exposed persons and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis (OJ L 214, p. 29). As a rule, public offices below the national level are not considered prominent public functions unless their political significance is comparable with those at the national level. Any person who has not held a prominent public function for at least a year shall no longer be considered politically exposed. Institutions or persons covered by this Act obligated to clarify whether the contracting party is a close associate of a person who has been entrusted with prominent public functions must do so only if this relationship is known to the public or if the institutions or persons covered by this Act have reason to believe that such a

relationship exists; they are however not obligated to conduct investigations. If the contracting party is a politically exposed person as defined here based outside the country, the following shall apply:

- a) establishing a business relationship through an intermediary acting on behalf of institutions or persons covered by this Act shall be subject to approval by his/her immediate supervisor or next-higher management level;
- b) appropriate measures shall be taken to determine the origin of assets to be used in the business relationship or transaction; and
- c) the business relationship shall be subject to continuous, enhanced oversight.

The contracting party shall provide the necessary information for the institutions and persons covered by this Act to fulfil their due diligence obligations and shall inform them of any changes without delay as long as they maintain a business relationship.

2. If the contracting party is a natural person who has not been physically present for identification purposes, institutions and persons covered by this act shall verify the contracting party's identity using a document as defined in Section 4 (4) first sentence no. 1, a certified copy of such a document, or a qualified digital signature as defined in Section 2 no. 3 of the Digital Signature Act and ensure that the first transaction is carried out through an account opened in the contracting party's name with a credit institution covered by Directive 2005/60/EC or a credit institution in a third country subject to requirements equivalent to those of this Act. If using a qualified digital signature to verify the contracting party's identity, institutions and persons covered by this Act shall check the validity of the certificate, the certification service provider report in accordance with Section 4 (3) of the Digital Signature Act, the integrity of the certificate and its relation to the signed data.

(3) In consultation with the Federal Ministry of Finance and the Federal Ministry of Economics and Technology, the Federal Ministry of the Interior may, by means of statutory instruments without the approval of the Bundesrat,

1. determine additional measures in the cases listed in paragraph 2 to be taken by institutions and persons covered by this Act in order to address the higher level of risk;
2. subject to implementation measures taken by the European Commission pursuant to Article 40 (1) c of Directive 2005/60/EC and to Article 13 (6) of this Directive, designate additional cases with a higher risk of money laundering or terrorist financing and define measures to be taken by institutions and persons covered by this Act in order to address the higher level of risk.

## Section 7

### Performance by third parties

(1) The institutions and persons covered by this Act may rely on third parties to meet the due diligence requirements laid down in Section 3 (1) nos. 1 through 3. However, the ultimate responsibility for meeting those requirements remains with the institution or person covered by this Act. For the purposes of this Act, "third parties" shall mean institutions and persons in the European Union Member States as defined in Section 2 (1) nos. 1,4,5,7 and 8 as well as Section 2 (1) no. 2 if they are financial services institutions as defined in Section 1 (1a) second sentence nos. 1, 2 through 5 and 8 of the Banking Act. If they are subject to mandatory registration or permission for their business or professional activity, apply due diligence requirements and record-keeping requirements equivalent to those laid down in Directive 2005/60/EC, and are supervised accordingly, third parties shall also include credit institutions, lawyers, notaries, auditors and tax advisers as well as insurance companies situated in third countries if they conduct business covered by Directive 2002/83/EC or provide accident insurance with premium redemption. If a third party in another European Union Member State carries out due diligence requirements equivalent to those laid down in Section 3 (1) nos. 1 through 3, fulfilling the Member State's law on information to be gathered and verified documents suffice. In the cases described in this paragraph, third parties shall

immediately forward to the institutions and persons covered by this Act the information gathered during measures equivalent to those laid down in Section 3 (1) nos. 1 through 3; at the request of such institutions and persons, third parties shall also forward copies of identification data and other relevant documentation on the identity of the contracting party or the beneficial owner.

(2) The institutions and persons covered by this Act may assign, on the basis of a contractual arrangement, another person to carry out the measures necessary to meet the due diligence requirements laid down in Section 3 (1) nos. 1 through 3. Doing so shall not prevent the institutions and persons covered by this Act from properly performing their duties as laid down by this Act, nor interfere with supervision or oversight by the directors of such institutions and persons, nor interfere with auditing rights or oversight by the responsible authority in accordance with Section 16 (2) with regard to the institutions and persons covered by this Act. Before collaborating with a third party, such institutions and persons shall be satisfied as to the reliability of that party and shall take random samples during their collaboration to verify the appropriateness and propriety of the measures taken by the third party. The measures taken by the third party are legally attributed to the institution or person covered by this Act. Section 25a (2) of the Banking Act shall remain unaffected.

(3) In consultation with the Federal Ministry of Finance and the Federal Ministry of Economics and Technology, the Federal Ministry of the Interior may, by means of statutory regulation without the approval of the Bundesrat and to implement a decision of the European Commission pursuant to Article 40 (4) of Directive 2005/60/EC, determine exceptions to paragraph 1 allowing institutions and persons covered by this Act to rely on third parties located outside the European Union to meet due diligence requirements.

## Section 8

### Record-keeping

(1) Where due diligence is required by this Act, collected data and information gathered on contracting parties, economic beneficiaries, business relationships and transactions shall be recorded. In the cases referred to in Section 4 (4) first sentence no. 1, the type, number and issuing authority of the document presented to verify identity shall also be recorded. A copy of the document presented to verify identity pursuant to Section 4 (4) first sentence no. 1 or no. 2 shall qualify as a record of the information contained in the document; in case of an inspection of electronically kept register data a copy of the print-out shall qualify as a record of the information contained in the print-out. If repeat verification of identity is waived under Section 4 (2), the name of the person who is to be identified and the fact that the person was previously identified shall be recorded. Where in the case of Section 6 (2) no. 2 a natural person has been identified using a qualified digital signature and that signature has been subject to appropriate verification, the fact that such verification was carried out shall be recorded.

(2) The records may also be stored on an image recording or other data storage medium. Measures shall be taken to ensure that the recorded data agree with the information gathered, are available during the retention period and can be made available at any time for reading given reasonable advance notice.

(3) The records as defined in paragraph 1 and other evidence pertaining to business relationships and transactions shall be kept for at least five years, without prejudice to other legal provisions. In the case of Section 3 (2) first sentence no. 1, the retention period shall begin at the end of the calendar year in which the business relationship with the contracting party was terminated. In all other cases, it shall begin at the end of the calendar year in which the information was obtained.

(4) Where records subject to retention must be presented to a public agency, Section 147 (5) of the German Fiscal Code shall apply as appropriate.



## Section 9

## Internal safeguards

(1) Institutions and persons as defined in Section 2 (1) must take appropriate internal measures to ensure that they cannot be misused for the purpose of money laundering and terrorist financing. For institutions and persons as defined in Section 2 (1) no. 7, this shall apply only where they conduct the transactions listed there on a regular basis.

(2) For the purposes of paragraph 1, “internal safeguard” means

1. for institutions and persons as defined in Section 2 (1) nos. 1, 2 and 4: designating a compliance officer (money laundering) directly subordinate to the management to act as contact for the law enforcement authorities and for the Federal Criminal Police Office – Financial Intelligence Unit – as well as for competent authorities referred to in Section 16 (2); for institutions and persons as defined in Section 2 (1) nos. 1 and 2 as higher-level companies this shall also apply to groups of institutions as defined in Section 10a (1) or (2) of the Banking Act and to financial holding groups as defined in Section 10a (3) of the Banking Act and as a parent company also to financial conglomerates as defined in Section 1 (20) first sentence of the Banking Act; for institutions and persons as defined in Section 2 (1) no. 4 as parent companies this shall also apply to insurance holding companies as defined in Section 104a (2) no. 4 of the Act on the Supervision of the Insurance Industry, to mixed insurance holding companies as defined in Section 104a (2) no. 5 or Section 104k no. 3 of the Act on the Supervision of the Insurance Industry, and to financial conglomerates as defined in Section 104k no. 4 of the Act on the Supervision of the Insurance Industry where the subsidiaries conduct business covered by Directive 2002/83/EC or offer accident insurance with premium redemption; such institutions and persons shall provide the means and procedures necessary for the compliance officer (money laundering) to carry out his/her responsibilities properly and effectively;
2. developing and updating internal principles, appropriate business and customer-related safeguards and controls to prevent money laundering and terrorist financing;
3. ensuring that employees responsible for carrying out transactions and for initiating and establishing business relationships are aware of methods of money laundering and terrorist financing and of the requirements pursuant to this Act.

(3) Where a natural person falling within any of the categories listed in Section 2 (1) nos. 7 to 10 or no. 12 performs his/her professional activities as an employee of a legal person, the obligations in paragraph 1 shall apply to that legal person rather than to the natural person. Institutions and persons covered by paragraph 1 may assign third parties, on the basis of a contractual arrangement, to carry out internal safeguards as defined in paragraph 2, record-keeping as defined in Section 8 and, where applied, internal safeguards as defined in Section 25c (2) of the Banking Act and Section 80d (1) of the Act on the Supervision of the Insurance Industry with the prior approval of the competent authorities pursuant to Section 16 (2). Such approval may be given only when the third party guarantees that it will carry out the measures properly and that management by the institution and person covered by the Act and supervision by the competent authority pursuant to Section 16 (2) will not be affected.

(4) In individual cases, the competent authority pursuant to Section 16 (2) may give instructions that are appropriate and necessary to implement the internal safeguards as defined in paragraph 2 no. 2. The authority may allow the obligations in paragraphs 1 and 2 to be applied to individual or groups of institutions or persons as defined in Section 2 (1) on a risk-sensitive basis due to the type and amount of business conducted by such individuals or groups. By way of derogation from the first sentence, the German Federal Bar shall give such instructions for lawyers and legal advisers who are members of a chamber of lawyers; the federal chamber of tax advisers for tax advisers and tax agents; the federal



chamber of notaries for notaries who are members of a chamber of notaries; and the competent supreme *Land* authority pursuant to Section 11 (4) fourth sentence for notaries who do not belong to a chamber of notaries.

### Chapter 3

#### Financial Intelligence Unit, reporting requirements and use of data

##### Section 10

##### Financial Intelligence Unit

(1) As central agency within the meaning of Section 2 (1) of the Federal Criminal Police Office Act, the Federal Criminal Police Office - Financial Intelligence Unit - shall support the federal and state (*Länder*) police forces in the prevention and prosecution of money laundering and terrorist financing. The Federal Criminal Police Office - Financial Intelligence Unit - shall

1. collect and analyse suspicious transaction reports transmitted pursuant to Sections 11 and 14, and in particular arrange for the cross-checking of data stored by other agencies;
2. inform the federal and state law enforcement authorities of information concerning them and on the facts of the crimes ascertained,
3. maintain the statistics as described in Article 33 (2) of Directive 2005/60/EC;
4. publish an annual report; and
5. regularly inform the persons obliged to report on types and methods of money laundering and terrorist financing.

(2) The Federal Criminal Police Office - Financial Intelligence Unit - shall co-operate with the financial intelligence units of other states responsible for the prevention and prosecution of money laundering and terrorist financing. It is the financial intelligence unit as defined in Article 2 (3) of the Council Decision (2000/642/JHA) of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (OJ L 271, p. 4).

(3) Where necessary for the performance of its duties pursuant to paragraphs 1 and 2, the Federal Criminal Police Office - Financial Intelligence Unit - may collect, process and use personal data in accordance with Sections 7 to 14 and Sections 27 to 37 of the Federal Criminal Police Act. In Section 7 (2) of the Federal Criminal Police Act, the duties listed in paragraphs 1 and 2 shall replace the duty as central unit pursuant to Section 2 (2) no. 1 of the Federal Criminal Police Act. Section 14 (1) of the Federal Criminal Police Act shall be applied with the proviso that transmission to the other countries' financial intelligence units is allowed. The Federal Criminal Police Office - Financial Intelligence Unit - may request information from the Federal Financial Supervisory Authority (BAFin) pursuant to Section 24c (3) first sentence no 2 of the Banking Act where necessary to perform its duties in accordance with paragraphs 1 and 2.

(4) The Federal Criminal Police Office - Financial Intelligence Unit - may use data provided by the financial intelligence unit of another country solely in line with the conditions imposed by the financial intelligence unit which provided the data. It may impose its own restrictions and conditions on the use of information transmitted to the financial intelligence unit of another country.

##### Section 11

##### Suspicious transaction reports

(1) Regardless of the amount involved, institutions and persons covered by this Act who have reason to believe that an offence under Section 261 of the Criminal Code or that terrorist financing has been or will be committed or attempted shall immediately inform the competent law enforcement agency orally, in

writing or via electronic data transmission, with a copy to the Federal Criminal Police Office – Financial Intelligence Unit. A requested transaction shall not be executed before the public prosecutor's office has informed the institution or person covered by this Act of its consent, or before the end of the second working day following the transmission of such report without this transaction having been prohibited under the Code of Criminal Procedure (StPO); Saturday shall not be considered a working day in this respect. If it is impossible to postpone the transaction, or if doing so could hinder efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, the institutions and persons concerned may carry out the transaction and shall inform the FIU immediately afterwards.

(2) A report originally made orally or over the telephone pursuant to paragraph 1 shall be repeated in written form, including telex and electronic data transmission.

(3) By way of derogation from paragraph 1 first sentence, the persons referred to in Section 2 (1) nos. 7 and 8 are not obliged to make a report if their suspicion is based on information from or about their client obtained while providing legal advice or legal representation in court for this client. The obligation to report shall remain in effect if the persons referred to in the first sentence know that their client is deliberately using their legal advice for the purpose of money laundering or terrorist financing.

(4) By way of derogation from paragraph 1 first sentence, where the persons referred to in Section 2 (1) nos. 7 and 8 are members of a professional chamber, they shall transmit the report to the competent federal professional chamber. Such chamber may comment on the report. It shall immediately transmit the report with its comments in accordance with paragraph 1 first sentence to the parties referred to therein. For notaries who are not members of a chamber of notaries, the highest *Land* authority responsible for the regulation of their profession shall take the place of the federal chamber of notaries.

(5) The obligation to report pursuant to paragraphs 1 and 2 does not rule out the voluntary character of the notification within the meaning of Section 261 (9) of the Criminal Code.

(6) The contents of a report pursuant to paragraph 1 may be used only for the criminal proceedings specified in Section 15 (1) and (2) third sentence, for criminal proceedings related to a criminal offence liable to maximum punishment of more than three years of imprisonment, for taxation proceedings, for the supervisory tasks of competent authorities pursuant to Section 16 (2) and for the purpose of threat prevention.

(7) In order to combat money laundering and terrorist financing, the Federal Ministry of the Interior and the Federal Ministry of Finance may, via statutory regulation with the approval of the Bundesrat, define individual types of financial transactions deemed to be suspicious within the meaning of paragraph 1 first sentence and which must be reported by the institutions and persons covered by this Act. The statutory regulation is to be limited in time.

(8) In criminal proceedings where a report has been made pursuant to paragraph 1 or Section 14, and in other criminal proceedings on suspicion of an offence pursuant to Section 261 of the Criminal Code or in which suspected offences pursuant to Section 1 (2) are being investigated, the competent public prosecutor's office shall inform the Federal Criminal Police Office - Financial Intelligence Unit - of the commencement and the outcome of proceedings. This shall take the form of sending a copy of the indictment, the reason for dismissal or the verdict. Institutions or persons covered by this Act who made a report pursuant to paragraph 1 may be given information from the files at their request in accordance with Section 475 of the Code of Criminal Procedure where necessary to check their report; Section 477 (3) of the Code of Criminal Procedure shall not apply in this respect. Institutions or persons covered by this Act may use personal data obtained pursuant to the third sentence only to check their report and must destroy this data when no longer needed for this purpose.

## Section 12

### Prohibition of disclosure

(1) Institutions and persons covered by this Act shall not disclose to the customer concerned or to other third persons the fact that information has been transmitted in accordance with Section 11 (1) or that an investigation is being carried out. This shall not apply to disclosure

1. to state agencies and the competent authorities referred to in Section 16 (2);
2. between institutions and persons which belong to the same group of institutions as referred to in Section 10a (1) or (2) of the Banking Act, the same financial holding group as referred to in Section 10a (3) of the Banking Act, the same financial conglomerate as referred to in Section 1 (20) first sentence of the Banking Act, the same insurance holding company as referred to in Section 104a (2) no. 4 of the Act on the Supervision of the Insurance Industry or the same mixed insurance holding as referred to in Section 104a (2) no. 5 or 104k no. 3 of the Act on the Supervision of the Insurance Industry, or the same financial conglomerate as referred to in Section 104k no. 4 of the Act on the Supervision of the Insurance Industry in European Union Member States or in third countries subject to requirements equivalent to those of Directive 2005/60/EC and supervised for compliance with those requirements;
3. between institutions and persons as defined in Section 2 (1) nos. 7 and 8 from European Member States or from third countries subject to requirements equivalent to those of Directive 2005/60/EC, where such persons are self-employed or employed by the same legal person or within a structure having a joint owner or management or joint supervision of compliance with requirements to prevent money laundering and terrorist financing;
4. between institutions or persons referred to in Section 2 (1) nos. 1 to 8 in cases related to the same contracting party and the same transaction involving two or more institutions or persons, provided that they are situated in a European Union Member State, or in a third country which imposes requirements equivalent to those laid down in Directive 2005/60/EC, and that they are from the same professional category and are subject to equivalent obligations as regards professional secrecy and personal data protection.

Information disclosed pursuant to the second sentence may be used solely for the purpose of preventing money laundering or terrorist financing.

(2) Where the persons referred to in Section 2 (1) nos. 7 and 8 seek to dissuade a client from engaging in illegal activity, this shall not constitute disclosure.

(3) In individual cases, institutions or persons referred to in Section 2 (1) nos. 1 to 6 may provide each other with information other than that listed in paragraph 1 first sentence when carrying out their due diligence requirements under Sections 3, 5 and 6, Sections 25d and 25f of the Banking Act and Section 80e of the Act on the Supervision of the Insurance Industry, where a suspicious or unusual transaction related to money laundering or terrorist financing is concerned and there is reason to believe that the recipient needs the information to decide whether to report the matter pursuant to Section 11 or to press charges in accordance with Section 158 of the Code of Criminal Procedure. The recipient may use the information solely for the purpose of preventing money laundering or terrorist financing and only under the conditions stipulated by the institution or person providing the information.

(4) In consultation with the Federal Ministry of Finance and the Federal Ministry of Economics and Technology, the Federal Ministry of the Interior may, by means of statutory regulation without the approval of the Bundesrat and to implement a decision of the European Commission pursuant to Article 40 (4) of Directive 2005/60/EC, determine further regulations prohibiting disclosure and determine to which institutions and persons in third countries no information may be disclosed.

### Section 13

#### Release from responsibility

- (1) Anyone who reports to the law enforcement authorities facts suggesting a criminal offence pursuant to Section 261 of the Criminal Code or terrorist financing cannot be held responsible for such report unless the report has been made in a deliberately or grossly negligently false manner.
- (2) The same shall apply to any employee who reports suspicious activity to his/her supervisor or to an in-house unit for the reporting of such activity.

### Section 14

#### Suspicious transaction reports filed by government authorities

- (1) Where they have reason to believe that an offence under Section 261 of the Criminal Code or that terrorist financing has been or will be committed or attempted, the competent authorities referred to in Section 16 (2) shall immediately inform the competent law enforcement agency, with a copy to the Federal Criminal Police Office – Financial Intelligence Unit.
- (2) Where they have reason to believe that an offence under Section 261 of the Criminal Code or that terrorist financing has been or will be committed or attempted, the finance administration authorities responsible for oversight of cross-border traffic and for monitoring the stock, foreign exchange and financial derivatives markets shall immediately inform the competent law enforcement agency, with a copy to the Federal Criminal Police Office – Financial Intelligence Unit.

### Section 15

#### Reference to and use of records

- (1) Records made pursuant to Section 8 (1) may be referred to or used for prosecuting criminal offences pursuant to Section 261 of the Criminal Code or criminal offences referred to in Section 129a (2) or Section 261 (1) of the Criminal Code.
- (2) Where criminal proceedings are initiated due to a criminal offence referred to in paragraph 1, the tax authorities shall be notified of this fact, together with the underlying facts, as soon as a financial transaction has been identified which could be important for the tax authorities to initiate or conduct tax assessment or tax-related criminal proceedings. If the law enforcement authority uses records referred to in Section 8 (1) in the criminal proceedings, these records may also be transmitted to the tax authorities. Notifications and records may be used for tax assessment and for tax-related criminal proceedings.

## Chapter 4 Supervision and administrative fines

### Section 16 Supervision

(1) The authorities referred to in paragraph 2 shall be responsible for supervision of the institutions and persons referred to in Section 2 (1). Within the framework of their legally assigned duties, the competent authorities may take the appropriate and necessary measures and orders to ensure compliance with the requirements of this Act. To do so, they may exercise the authority granted them for other supervisory tasks.

(2) The competent authority for enforcing this Act shall be

1. for the Development Loan Corporation (Kreditanstalt für Wiederaufbau): the Federal Ministry of Finance;
2. for all other credit institutions (excepting the German Bundesbank), financial services institutions, domestic branches of credit institutions and financial services institutions with head offices abroad, investment companies as defined in Section 2 (5) of the Investment Act and investment management companies as defined in Section 2 (6) of the Investment Act: the Federal Financial Supervisory Authority (BaFin);
3. for insurance companies and the domestic branches of such companies: the competent supervisory authority for the insurance industry;
4. for lawyers and legal advisers who are members of a chamber of lawyers: the competent bar association (Sections 60 and 61 of the Federal Statute on Attorneys (BRAO));
5. for patent lawyers: the chamber of patent lawyers (Section 53 of the Federal Statute on Patent Lawyers (PatAnwO));
6. for notaries: the president of the regional court of the district where the notary is based (Section 92 no. 1 of the Federal Statute on Notaries (BNotO));
7. for auditors and chartered accountants: the Chamber of Auditors (Section 57 (2) no. 17 of the Federal Statute on Auditors (WiPrO));
8. for tax advisers and tax agents: the competent chamber of tax advisers (Section 76 of the Act on Tax Advising (StBerG));
9. for all others: the authority responsible under federal or state (*Land*) law.

### Section 17 Administrative fines

(1) Anyone who intentionally or negligently commits one of the following shall be deemed to have committed an administrative offence:

1. fails to identify a contracting party in violation of Section 3 (1) no. 1;
2. fails to record information correctly or completely in violation of Section 8 (1);
3. fails to keep records and other evidence of business relationships and transactions in violation of Section 8 (3); or
4. fails to report suspicious activity in violation of Section 11 (1).

(2) Anyone who commits one of the following shall be deemed to have committed an administrative offence:

1. in violation of Section 3 (1) no. 3 fails to clarify whether the contracting party is acting on behalf of a beneficial owner;
2. in violation of Section 4 (5) first sentence fails to find out the name of the beneficial owner;

3. in violation of Section 6 (2) no. 2 fails to verify the identity of a contracting party or fails to ensure that the first transaction is carried out through an account opened in the contracting party's name; or
4. in violation of Section 12 (1) discloses information to the customer concerned or to institutions or persons other than those referred to in Section 12 (1) second sentence.

(3) In the cases referred to in paragraph 1, the administrative offence may be punished by a fine of up to EUR 100 000; in the cases referred to in paragraph 2 by a fine of up to EUR 50 000.

(4) The authority designated in Section 16 (2) nos. 2 and 3 shall also be the administrative authority as defined in Section 36 (1) no. 1 of the Act on Administrative Offences (OWiG). For tax consultants and tax agents, the tax office (*Finanzamt*) shall be the administrative authority as defined in Section 36 (1) no. 1 of the Act on Administrative Offences. Where the competent unit under federal or state (*Land*) law is the authority designated in Section 16 (2) no. 9, it shall also be the administrative authority as defined in Section 36 (1) no. 1 of the Act on Administrative Offences.

(5) Where the tax office is the administrative authority as defined in paragraph 4 second sentence, Section 387 (2), Section 410 (1) nos. 1, 2, 6 to 11, (2) and Section 412 of the Fiscal Code shall apply *mutatis mutandis*.

### Article 3

#### Amendment of the Banking Act

The Banking Act as published on 9 September 1998 (Federal Law Gazette I, p. 2776), last amended by Article 2 of the Act of 21 December 2007 (Federal Law Gazette I, p. 3081), shall be amended as follows:

1. The table of contents shall be amended as follows:

a) After the information on Section 25a, the following sub-heading shall be inserted:

“5a. Prevention of money laundering, terrorist financing and fraudulent activity to the detriment of the institutions”

b) After the reference to Section 25b, the following information shall be inserted:

“Section 25c	Internal safeguards
Section 25d	Simplified due diligence
Section 25e	Simplified identification
Section 25f	Enhanced due diligence
Section 25g	Group compliance with due diligence requirements
Section 25h	Prohibited transactions”

c) In the sub-heading above Section 26, “5a” shall be replaced with “5b”.

d) In the sub-heading above Section 26a, “5b” shall be replaced by “5c”.

2. Section 24c shall be amended as follows:

a) Paragraph 1 first sentence no. 2 shall read as follows:



“2. The name, and in the case of natural persons the date of birth, of the account holder and any person with the right of disposal and, in the cases of Section 3 (1) no. 3 of the Money Laundering Act the name, and if registered, the address of any beneficial owner not being the customer or contractual partner as defined in Section 1 (6) of the Money Laundering Act.”

b) Paragraph 8 shall read as follows:

“(8) Where the German Bundesbank and the Federal Republic of Germany – Finance Agency GmbH manage accounts and deposits for third parties, they shall be deemed credit institutions as defined in paragraphs 1, 5 and 6.”

3. Section 25a (1) sixth sentence shall be amended as follows:

a) The semicolon at the end of no. 2 shall be replaced by a full stop.

b) No. 3 shall be deleted.

4. Section 25b shall be preceded by the following sub-heading:

“5a. Prevention of money laundering, terrorist financing and fraudulent activity to the detriment of institutions”

5. The following Sections 25c to 25h shall be inserted after Section 25b:

“Section 25c  
Internal safeguards

(1) Without prejudice to the requirements listed in Section 25a (1) of this Act and in Section 9 (1) and (2) of the Money Laundering Act and in the framework of their orderly business organization and appropriate risk management, institutions shall develop and update internal principles, appropriate business and customer-related safeguards and controls and perform inspections to prevent fraudulent activity.

(2) Credit institutions shall operate and update appropriate data processing systems which enable them to recognize business relationships and individual transactions that should be regarded as suspicious or unusual on the basis of experience and knowledge generally and specifically available within the credit institution concerning methods of money laundering, terrorist financing and fraudulent activity to the detriment of institutions. Where such activity is detected, it shall be investigated in the context of the ongoing business relationship and individual transactions in order to be able to monitor and assess the risk of these business relationships and transactions and to determine whether it constitutes suspicious activity. Credit institutions may gather, process and use personal data as needed to meet this obligation. The Federal Financial Supervisory Authority (BAFin) can define criteria for cases in which credit institutions are not required to use systems referred to in the first sentence.

Section 25d  
Simplified due diligence

(1) Where the conditions laid down in Section 25f of this Act and in Section 6 of the Money Laundering Act are not met, institutions face a low risk of money laundering or terrorist financing in the following cases beyond those listed in Section 5 of the Money Laundering Act:

1. when issuing or managing electronic money as defined in Section 1 (14), as long as it is guaranteed that
  - a) if the data storage device cannot be recharged, the maximum amount stored in the device is no more than EUR 150; or
  - b) if the data storage device can be recharged, a limit of EUR 2 500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1 000 or more is redeemed in that same calendar year by the bearer as referred to in Section 22p (1);
2. subject to the second sentence when concluding
  - a) a contract for a state subsidized, fully funded private pension;
  - b) a contract for capital-forming investment, where the contract meets the conditions for state subsidies;
  - c) a loan contract, financial leasing contract or instalment sale transaction with a consumer (Sections 491, 500, 501 of the Civil Code (BGB));
  - d) a loan contract as part of a state subsidy programme carried out by a federal or state development bank, where the loan amount must be used for a designated purpose;
  - e) credit contract for instalment financing;
  - f) any other loan contract where the loan account serves the exclusive purpose of repaying the loan and the loan payments are withdrawn from the creditor's account with a credit institution as defined in Section 1 (1) (with the exception of those companies referred to in Section 2 (1) nos. 3 to 8), with a credit institution in another European Union Member State or with a domestic branch of a credit institution having its head office abroad;
  - g) a savings agreement; and
  - h) a leasing agreement;
3. subject to the second sentence in other cases where the following conditions are met:
  - a) the contract is in writing;
  - b) the relevant transactions are carried out using the customer's account with a credit institution as defined in Section 1 (1) (with the exception of those companies referred to in Section 2 (1) nos. 3 to 8), with a credit institution in another European Union Member State, with a domestic branch of a credit institution having its head office abroad, or with a credit institution located in a third country and subject to requirements equivalent to those in Directive 2005/60/EC;
  - c) the product or related transaction is not anonymous and allows for the timely application of Section 3 (2) first sentence no. 3 of the Money Laundering Act; and
  - d) the benefits from the contract or related transaction cannot be paid to third parties except in case of death, disability, exceeding a certain age limit or similar cases;
4. subject to the second sentence where products or related transactions in which it is possible to invest in financial investments or claims such as insurance or other contingent claims where in addition to the conditions laid down in no. 3
  - a) benefits from the product or transaction may be paid out only over the long term;
  - b) the product or transaction cannot be deposited as a security; and
  - c) no early payments can be made and no repurchase clauses can be claimed and the contract cannot be terminated before its date of maturity.

In the cases of the first sentence nos. 2 to 4, a low risk shall be deemed to exist only where the following threshold values are not exceeded:

1. for contracts referred to in the first sentence no. 2 ad a, b, d and f or for contracts referred to in the first sentence no. 3 and 4 a total of EUR 15 000 in payments;
2. for contracts referred to in the first sentence no. 2 ad c, e and h or for other contracts to finance goods or their use and where the property title is not transferred to the contracting party or user until all instalments have been paid, EUR 15 000 in payments per calendar year;
3. for savings agreements referred to in the first sentence no. 2 ad g with periodical payments of EUR 1 000 per calendar year or a one-time payment of EUR 2 500.

(2) Paragraph 1 shall not apply when the institutions or persons covered by this Act have information about a specific transaction or business relationship indicating a higher risk of money laundering or terrorist financing.

#### Section 25e Simplified identification

By way of derogation from Section 4 (1) of the Money Laundering Act, the identity of the contracting party and the beneficial owner may also be verified immediately after an account or deposit is opened. In this case it is necessary to ensure that no funds can be diverted from the account or deposit before the verification of identity is complete.

#### Section 25f Enhanced due diligence

(1) In addition to the requirements referred to in Section 6 of the Money Laundering Act, institutions shall apply enhanced due diligence measures appropriate to higher-risk transactions as part of business relationships with respondent institutions based in third countries. Where these business relationships are not related to the processing of transactions, Section 5 (2) no. 1 of the Money Laundering Act shall remain unaffected. Section 3 (4) second sentence of the Money Laundering Act shall apply *mutatis mutandis*.

(2) In the cases referred to in paragraph 1, institutes shall

1. both before establishing such a business relationship and during such a relationship, gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and management structure to determine from publicly available information the reputation of the institution and the quality of supervision to assess the respondent institution's controls to prevent money laundering and terrorist financing;
2. before establishing such relationships, define and document the respective responsibilities of each institution with respect to meeting due diligence requirements;
3. before establishing such a relationship through an intermediary acting on behalf of institutions or persons covered by this Act, obtain approval from the immediate supervisor or next-higher management level;
4. take measures to ensure that the respondent institution does not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank as defined in Article 3 (10) of Directive 2005/60/EC of the European Parliament and the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJ L 309, p. 15), last amended by Directive 2007/64/EC of the European Parliament and the Council of 13 November 2007 (OJ L 319, p. 1); and
5. take measures to ensure that respondent institutions do not allow transactions via payable-through accounts.

(3) By way of derogation from Section 3 (2) first sentence no. 2 of the Money Laundering Act, institutions and persons referred to in Section 2 (1) nos. 1 and 2 of the Money Laundering Act shall remain responsible for due diligence requirements laid down in Section 3 (1) nos. 1 and 3 of the Money Laundering Act when accepting cash regardless of any threshold amounts stated in the Money Laundering Act or in this Act where a money transfer as defined in Section 1 (1a) second sentence no. 6 or currency exchange transaction as defined in Section 1 (1a) second sentence no. 7 requested by a customer is carried out through an account other than the customer's account with the institution or person covered by this Act and the value of a transaction in case of a currency exchange transaction is or exceeds EUR 2500.

## Section 25g

## Group compliance with due diligence requirements

Institutions that are higher-level companies within an institutional group as defined in Section 10a (1) or (2), a financial holding group as defined in Section 10a (3) or a parent company of a financial conglomerate as defined in Section 1 (20) first sentence shall create internal safeguards as referred to in Section 9 of the Money Laundering Act and Section 25c (1) for their branches and majority-owned subsidiaries and ensure compliance with due diligence requirements referred to in Sections 3, 5 and 6 of the Money Laundering Act and Sections 25d and 25f as well as the recording and retention requirements referred to in Section 8 of the Money Laundering Act, where permitted by the legislation of the country in which the branch or company is located. Senior management as defined in Section 1 (2) first sentence shall be responsible for ensuring that the requirements referred to in the first sentence are properly met. In cases where the legislation of the third country where the company is located does not permit application of the measures required under the first sentence, the higher-level company or parent company shall immediately inform the Federal Financial Supervisory Authority (BAFin) and take additional measures to effectively handle an enhanced risk of money laundering or terrorist financing. If stricter requirements apply in the third country in which the branch or company is located, these requirements shall be met in that country.

## Section 25h

## Prohibited transactions

The following shall be prohibited:

1. initiating or continuing a correspondent or other business relationship with a shell bank as defined in Article 3 no. 10 of Directive 2005/60/EC; and
  2. establishing or managing accounts in the institution's name or for third-party institutions which customers may access independently to carry out their own transactions; Section 154 (1) of the German Fiscal Code shall remain unaffected."
6. In the sub-heading above Section 26, "5a" shall be replaced by "5b", and in the sub-heading above Section 26a, "5b" shall be replaced by "5c".
  7. In Section 29 (2) first sentence, the reference "Section 25a (1) sixth sentence no. 3" shall be replaced by the reference "25c to 25h".
  8. Section 53b (3) first sentence shall be amended as follows:
 

"The following regulations shall be applied to branches as defined in paragraph 1 first and second sentences accordingly, with the proviso that one or more branches of the same company shall be regarded as one credit institution, e-money institution or financial services institution:

    1. Sections 3 and 6 (2);
    2. Section 11, where the institution in question is an deposit-taking credit institution;
    3. Sections 14, 22 and 23;
    4. Section 23a, where the institution in question is an deposit-taking credit institution or financial services institution;
    5. Section 24 (1) nos. 5 and 7;
    6. Sections 24b, 24c, 25, 25a (1) sixth sentence no. 2;
    7. Section 25c (2), where requirements for the internal organization to prevent money laundering and terrorist financing are concerned;
    8. Sections 25d to 25f, Section 25h, Sections 37, 39 to 42, Section 43 (2) and (3), Section 44 (1) and (6), Section 44a (1) and (2), and Sections 44c, 46 to 49; and
    9. Section 17 of the Act on Financial Services Supervision (FinDAG)."

9. Section 56 shall be amended as follows:

a) In paragraph 3, the following nos. 7c and 7d shall be inserted after no. 7b:

“7c. establishes or continues a correspondent or other business relationship with a shell bank in violation of Section 25h no. 1;

7d.establishes or maintains an account in violation of Section 25h no. 2;”

b) The following paragraph 4 shall be inserted:

“(4) Persons shall be deemed to have committed an administrative offence if they violate Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds (OJ L 345, p. 1) by intentionally or negligently

1. failing to ensure that transfers of funds are accompanied by complete information on the payer, in violation of Article 5 (1);

2. failing to verify the complete information on the payer or to do so in a timely fashion, in violation of Article 5 (2) also in conjunction with (4);

3. failing to ensure that transfers of funds are accompanied by complete and accurate information on the payer, in violation of Article 7 (1);

4. failing to have effective procedures in place in order to detect whether the required information on the payer is missing, in violation of Article 8 second sentence;

5. failing to reject the transfer or ask for complete information on the payer, or to do either in a timely fashion, in violation of Article 9 (1) first sentence;

6. failing to keep records of any information received on the payer for at least five years, in violation of Articles 11 or 13 (5); or

7. failing to ensure that all information received on the payer that accompanies a transfer of funds is kept with the transfer, in violation of Article 12.”

c) Paragraph 4 shall become paragraph 5.

#### **Article 4**

#### **Amendment to the Act on the Supervision of the Insurance Industry**

The Act on the Supervision of the Insurance Industry as published on 17 December 1992 (Federal Law Gazette 1993 I, p. 2), last amended by Article 11 of the Act of 28 May 2008 (Federal Law Gazette I, p. 874), shall be amended as follows:

1. The table of contents shall be amended as follows:

a) The following sub-heading shall be inserted after Section 80b:

“4. Measures to prevent money laundering and terrorist financing”

b) The following information shall be inserted after the new sub-heading 4:

“Section 80c	Obligated companies
Section 80d	Internal safeguards
Section 80e	Simplified due diligence
Section 80f	Simplified identification”

2. Section 57 shall be amended as follows:

a) In paragraph 1 first sentence, the words “as well as the requirements pursuant to Section 14 of the Money Laundering Act” shall be deleted.

b) The following paragraph 1a shall be added after paragraph 1:

“(1a) In the case of insurance companies as defined in Section 80c, the auditor shall also determine whether these have met the requirements referred to in Sections 80d to 80f and in the Money Laundering Act. The auditor shall report on this matter separately.”

3. The following sub-chapter shall be inserted after Section 80b:

“4. Measures to prevent money laundering and terrorist financing”

#### Section 80c

##### Obligated companies

The provisions in this sub-chapter shall apply to all insurance companies conducting business covered by Directive 2002/83/EC of the European Parliament and of the Council of 5 November 2002 concerning life assurance, or those providing accident insurance with premium redemption.

#### Section 80d

##### Internal safeguards

(1) Without prejudice to the requirements laid down in Section 9 (1) and (2) of the Money Laundering Act, insurance companies as defined in Section 80c shall operate and update appropriate systems which enable them to recognize business relationships and individual transactions that should be regarded as suspicious or unusual on the basis of experience and knowledge generally and specifically available within the insurance company concerning methods of money laundering and terrorist financing. Where such activity is detected, it shall be investigated in the context of the ongoing business relationship and individual transactions in order to be able to monitor and assess the risk of these business relationships and transactions and to determine whether it constitutes suspicious activity. Where they use data processing systems for this purpose, insurance companies may gather, process and use personal data as needed to meet this requirement.

(2) Where an insurance company as defined in Section 80c maintains an internal audit unit, this unit shall check compliance with requirements to prevent money laundering and terrorist financing at least once a year. The report of audit results shall be presented to the senior management, the money laundering commissioner and the supervisory authority.

(3) Insurance companies as defined in Section 80c that are parent companies within an insurance holding company as defined in Section 104a (2) no. 4, of a mixed insurance holding company as defined in Section 104a (2) no. 5 or Section 104a no. 3 or of a financial conglomerate as defined in Section 104k no. 4 shall create internal safeguards in accordance with paragraph 1 and Section 9 of the Money Laundering Act for their branches and majority-owned subsidiaries which offer contracts as defined in Section 80c and ensure compliance with due diligence requirements referred to in Sections 3, 5 and 6 of the Money Laundering Act and Section 80e as well as the recording and retention requirements referred to in Section 8 of the Money Laundering Act, where permitted by the legislation of the country in which the branch or company is located. Senior management as defined in Section 7a (1) fourth sentence shall be responsible for ensuring that the requirements referred to in the first sentence are properly met. In cases where the legislation of the third country where the company is located does not permit application of the measures



required under the first sentence, the higher-level company or parent company shall immediately inform the supervisory authority and take additional measures to effectively handle an enhanced risk of money laundering or terrorist financing. If stricter requirements apply in the third country in which the branch or company is located, these requirements shall be met in that country.

#### Section 80e

##### Simplified due diligence

(1) Where the conditions laid down in Section 6 of the Money Laundering Act are not met, insurance companies as defined in Section 80c face a low risk of money laundering or terrorist financing in the following cases beyond those listed in Section 5 of the Money Laundering Act:

1. in the case of contracts as defined in Section 80c, where the amount of premiums to be paid over one year does not exceed EUR 1 000 or where a one-time premium paid does not exceed EUR 2 500;
2. in the case of insurance policies for pension insurance contracts which neither contain a buy-back clause nor can serve as security for a loan;
3. in the case of pension schemes, plans or comparable systems providing pension benefits for employees, where contributions are deducted from employee pay and beneficiaries are not allowed to transfer their rights to third parties;
4. in all other cases where the following conditions are met:
  - a) the contract is in writing;
  - b) the relevant transactions are carried out using the customer's account with a credit institution as defined in Section 1 (1) of the Banking Act (with the exception of those companies referred to in Section 2 (1) nos. 3 to 8 of the Banking Act), with a credit institution in another European Union Member State, with a domestic branch of a credit institution having its head office abroad, or with a credit institution located in a third country and subject to requirements equivalent to those in Directive 2005/60/EC;
  - c) the product or related transaction is not anonymous and allows for the timely application of Section 3 (2) no. 3 of the Money Laundering Act;
  - d) the contract sets a threshold as defined in the first sentence no. 1; and
  - e) the benefits from the contract or related transaction cannot be paid to third parties except in case of death, disability, exceeding a certain age limit or similar cases;
5. in the case of products or related transactions in which it is possible to invest in financial investments or claims such as insurance or other contingent claims where, in addition to the conditions laid down in no. 4
  - a) benefits from the product or transaction may be paid out only over the long term;
  - b) the product or transaction cannot be deposited as a security; and
  - c) no early payments can be made and no repurchase clauses can be claimed and the contract cannot be terminated before its date of maturity.

(2) Paragraph 1 shall not apply when the insurance company has information about a specific transaction or business relationship indicating a higher risk of money laundering or terrorist financing.

#### Section 80f

##### Simplified identification

(1) By way of derogation from Section 4 (3) of the Money Laundering Act, the requirement to identify policy holders laid down in Section 3 (1) no. 1 of the Money Laundering Act shall be deemed to have been met where the policy holder authorizes the insurance company as defined in Section 80c to withdraw the premiums via direct debit from the policy holder's account with a credit institution having its

head office in a European Union Member State. If it is not possible to collect the premium from the account specified by the policy holder, the company shall identify the policy holder.

(2) Where an insurance policy contract concluded for an occupational pension on the basis of an employment contract or employment on the part of the policy holder contains an agreement that the premium is to be paid through the policy holder's account as specified in the contract, the requirement to identify the policy holder shall be deemed to be met if the insurance company confirms that the premium is actually paid through the agreed account.

(3) By way of derogation from Section 4 (1) of the Money Laundering Act, an insurance company as defined in Section 80c may also verify the identity of the beneficiary designated in the insurance policy after the business relationship has been established. In this case, verification must be completed before benefits are paid out or before the beneficiary intends to claim his/her rights granted by the insurance policy."

4. Section 83 (5) second sentence shall be amended as follows:

"In the cases referred to in no. 1, this shall apply only where relevant for the appraisal of the business and the assets of the insurance company, or for an insurance company as defined in Section 80c to meet the requirements laid down in Sections 80d to 80f or in the Money Laundering Act."

## Article 5

### Amendment of the Customs Administration Act

The Customs Administration Act (ZollVG) of 21 December 1992 (Federal Law Gazette I, p. 2125, 1993 I p. 2493), last amended by Article 8 of the Act of 13 December 2007 (Federal Law Gazette I, p. 2897) shall be amended as follows:

1. In paragraph 2 second sentence, the reference "Section 1 (4) of the Money Laundering Act" shall be replaced by the reference "Section 2 (1) nos. 1 to 6 of the Money Laundering Act of ... (Federal Law Gazette I, p. ... [*insert: date of signing, page number of promulgation and, if different, page number of Article 2 of the current amending act*] in the latest amended version".
2. Paragraph 5 shall be amended as follows:
  - a) In the second sentence, the words "as well as the Federal Financial Supervisory Authority (BAFin)" shall be inserted after the reference "Section 31b (3)".
  - b) The third sentence shall be amended as follows:
 

"Personal data may be transmitted to other tax authorities where their being informed may be important for carrying out

    1. tax-related administrative proceedings,
    2. criminal proceedings due to tax-related crime,
    3. a fine due to a tax-related administrative offence, or
    4. administrative proceedings due to prohibited financial transfer services."

## Article 6

### Amendment of the Investment Act

The Investment Act of 15 December 2003 (Federal Law Gazette I, p. 2676), last amended by Article 1 of the Act of 21 December 2007 (Federal Law Gazette I, p. 3089) shall be amended as follows:

1. Section 6 shall be amended as follows:
  - a) Paragraph 1 fourth sentence shall be deleted.
  - b) In paragraph 5, “and Sections 25c to 25h” shall be inserted after the reference “Section 24c”.
2. Section 99 (2) second sentence shall be deleted.

## Article 7

### Amendment of the Act on Financial Services Supervision

The Act on Financial Services Supervision of 22 April 2002 (Federal Law Gazette I, p. 1310), last amended by Article 6 of the Act of 21 December 2007 (Federal Law Gazette I, p. 3089) shall be amended as follows:

1. The following sentence shall be added after Section 14 (2) first sentence:
 

“Derogation from Section 15 of the Administrative Expenses Act (VwKostG) shall be permitted.”
2. In Section 17b (2) second sentence the reference “Section 14 (2) second sentence” shall be replaced by the reference “Section 14 (2) second and third sentences”.

## Article 8

### Amendment of the Ordinance on the imposition of fees and allocation of costs pursuant to the Act on Financial Services Supervision

In the Ordinance on the imposition of fees and allocation of costs pursuant to the Act on Financial Services Supervision (FinDAGKostV) of 29 April 2002 (Federal Law Gazette I, p. 1504, 1847), last amended by Article 7 of the Act of 21 December 2007 (Federal Law Gazette I, p. 3089), nos. 7.1 to 7.3 in the Annex to Section 2 (1) shall be replaced by the following:

“7.1	Ordinance to create internal safeguards as defined in Section 9 (2) no. 2 of the Money Laundering Act (GwG)  (Section 9 (4) first sentence GwG)	250
7.2	Ordinance on security measures necessary as the result of the internal risk situation  (Section 9 (4) second sentence GwG)	500”

## Article 9

### Amendment of the Ordinance on monthly financial statements

In Section 5 first sentence no. 3 of the Ordinance on monthly financial statements (MonAwV) of 31 May 1999 (Federal Law Gazette I, p. 1080, 1330), last amended by Article 3 (8) of the Act of 21 December

2000 (Federal Law Gazette I, p. 1857), the reference “of Section 2 of the Money Laundering Act” shall be replaced by “of EUR 15 000”.

## **Article 10**

### **Amendment of the Ordinance on auditors’ reports**

The Ordinance on auditors’ reports of insurance companies’ annual accounts (PrüfBV) of 17 December 1998 (Federal Law Gazette I, p. 3690) shall be amended as follows:

1. In Section 5 (1) no. 5 the reference “Section 14 (2) no. 1” shall be replaced by the reference “Section 9 (2) no. 1”.
2. Section 17 shall be amended as follows:
  - a) In paragraph 1 first sentence the reference “Section 2 (1) and (2) and Section 6” shall be replaced by the reference “Section 3 (2)”, the words “the identification of the beneficial owner” shall be replaced by the words “the requirement to clarify whether there is an beneficial owner and if so, to verify his/her identity”, and the words “have been met” shall be replaced by the words “have met”.
  - b) In Section 2 nos. 1 and 2 the reference “Section 14 (2) no. 1” shall be replaced by the reference “Section 9 (2) no. 1”.
  - c) Paragraph 2 no. 4 shall be deleted.
  - d) Paragraph 2 no. 5 shall become no. 4.

## **Article 11**

### **Entry into force, expiry**

This Act shall enter into force on the day after its promulgation. The Money Laundering Act of 25 October 1993 (Federal Law Gazette I p. 1770), last amended by Article 11 of the Act of 15 December 2003 (Federal Law Gazette I p. 2676, 2733) shall expire at the same time.

## **5. Commercial Code (*Handelsgesetzbuch, HGB*)**

(...)

## **Article 257**

### **Keeping of documents, periods of retention**

(1) Every merchant is obliged to keep the following documents in an organized manner:

1. books of account, inventories, opening balances, management reports, annual accounts, corporate accounts, corporate management report and all working instructions necessary for their understanding as well as further organisational documents,
2. the received trade letters,
3. copies of dispatched trade letters,
4. receipts for bookings in the records which he has to keep according to section 238 (1) (booking receipts)

(2) Trade letters are only such documents concerning a trading transaction.

(3) Except for opening balances, annual accounts and corporate accounts, the documents under subsection (1) may be stored as reproduction on an image recording or another data carrier if this corresponds to the General Accepted Accounting Principles and if it is guaranteed that the reproduction or the data stored

1. corresponds with the received trade letters and the receipts for bookings visually and the other documents in content when they are made readable,
2. is available during the retention-period and can at any time be made available for reading within an appropriate period of time.

If documents are produced on data carriers due to section 239 (4) sentence 1, the data may also be stored in printed form instead of storing the data carrier itself; the printed documents may also be stored according to sentence 1.

(4) The documents specified in subsection (1) nos. 1 and 4 shall be retained for 10 years, the other documents specified in subsection (1) for 6 years.

(5) The period of storage commences with the end of the calendar year in which the entry into the book of account was made, the inventory was compiled, the opening balance or the annual account was ascertained, the corporate account was compiled, the trade letter was received or dispatched, or the booking receipt was generated.

(...)

## **6. Administrative Offences Act (*Ordnungswidrigkeitengesetz, OWiG*)**

(...)

### **Article 30 Regulatory Fine Imposed on Legal Persons and on Associations of Persons**

(1) Where someone acting

1. as an entity authorised to represent a legal person or as a member of such an entity,
2. as chairman of the executive committee of an association without legal capacity or as a member of such committee,
3. as a partner authorised to represent a partnership with legal capacity, or
4. as the authorised representative with full power of attorney or in a managerial position as procura-holder or the authorised representative with a commercial power of attorney of a legal person or of an association of persons referred to in numbers 2 or 3,
5. as another person responsible on behalf of the management of the operation or enterprise forming part of a legal person, or of an association of persons referred to in numbers 2 or 3, also covering supervision of the conduct of business or other exercise of controlling powers in a managerial position, has committed a criminal offence or a regulatory offence as a result of which duties incumbent on the legal person or on the association of persons have been violated, or where the legal person or the association of persons has been enriched or was intended to be enriched, a regulatory fine may be imposed on such person or association.

(2) The regulatory fine shall amount

1. in the case of a criminal offence committed with intent, to not more than one million Euros,
2. in the case of a criminal offence committed negligently, to not more than five hundred thousand Euros.

Where there has been commission of a regulatory offence, the maximum regulatory fine that can be imposed shall be determined by the maximum regulatory fine imposable for the regulatory offence concerned. The second sentence shall also apply where there has been commission of an act

simultaneously constituting a criminal offence and a regulatory offence, provided that the maximum regulatory fine imposable for the regulatory offence exceeds the maximum pursuant to the first sentence.

(3) Section 17 subsection 4 and section 18 shall apply *mutatis mutandis*.

(4) If criminal proceedings or regulatory fining proceedings are not commenced on account of the criminal offence or of the regulatory offence, or if such proceedings are discontinued, or if imposition of a criminal penalty is dispensed with, the regulatory fine may be assessed independently. Statutory provision may be made to the effect that a regulatory fine may be imposed in its own right in further cases as well. Independent assessment of a regulatory fine against the legal person or association of persons shall however be precluded where the criminal offence or the regulatory offence cannot be prosecuted for legal reasons; section 33 subsection 1 second sentence shall remain unaffected.

(5) Assessment of a regulatory fine incurred by the legal person or association of persons shall, in respect of one and the same offence, preclude a forfeiture order, pursuant to sections 73 or 73a of the Penal Code or pursuant to section 29a, against such person or association of persons.

(...)

### **Article 36** Substantive Jurisdiction of the Administrative Authority

(1) Substantive jurisdiction shall lie with

1. the administrative authority designated by statute,
2. in the absence of such designation
  - a) the highest substantively competent *Land* authority, or
  - b) the substantively competent Federal Ministry as far as the law is implemented by Federal authorities.

(2) The *Land* government may, by means of a legal ordinance, delegate jurisdiction pursuant to subsection 1 number 2a, to another authority or agency. The *Land* government may delegate the authorisation to the highest *Land* authority.

(3) The Federal Ministry competent pursuant to subsection 1 number 2b may, by means of a legal ordinance that shall not require the approval of the *Bundesrat*, delegate its jurisdiction to another authority or agency.

(...)

### **Article 130**

(1) Whoever, as the owner of an operation or undertaking, intentionally or negligently omits to take the supervisory measures required to prevent contraventions, within the operation or undertaking, of duties incumbent on the owner as such and the violation of which carries a criminal penalty or a regulatory fine, shall be deemed to have committed a regulatory offence in a case where such contravention has been committed as would have been prevented, or made much more difficult, if there had been proper supervision. The required supervisory measures shall also comprise appointment, careful selection and surveillance of supervisory personnel.

(2) An operation or undertaking within the meaning of subsection 1 shall include a public enterprise.

(3) Where the breach of duty carries a criminal penalty, the regulatory offence may carry a regulatory fine not exceeding one million Euros. Where the breach of duty carries a regulatory fine, the maximum regulatory fine for breach of the duty of supervision shall be determined by the maximum



regulatory fine impossible for the breach of duty. The second sentence shall also apply in the case of a breach of duty carrying simultaneously a criminal penalty and a regulatory fine, provided that the maximum regulatory fine impossible for the breach of duty exceeds the maximum pursuant to the first sentence.

(...)

## **7. Banking Act (Kreditwesengesetz, KWG)**

(...)

### **Article 25a. Particular Organisational Duties of Institutions**

(1) An institution must have a proper business organisation which ensures compliance with the legal provisions to be adhered to by the institution. The persons listed in Section 1 Subsection 2 Sentence 1 are responsible for the proper business organisation of the institution. A proper business organisation shall encompass in particular

1. an appropriate strategy which also considers the risks and the own funds of the institution;
2. appropriate internal control procedures which consist of an internal control system and an internal auditing; the internal control system includes in particular suitable rules for the monitoring and controlling of risks;
3. appropriate rules by means of which the institution's financial situation can be assessed at any time with sufficient accuracy;
4. appropriate security precautions for the deployment of electronic data processing;
5. a complete documentation of the executed business transactions which permit a full and unbroken supervision by the Federal Financial Supervisory Authority for its area of responsibility; accounting vouchers shall be retained for ten years and other requisite records shall be retained for six years; Section 257 Subsections 3 and 5 of the Commercial Code applies accordingly;
6. appropriate, transaction and customer related systems securing against money laundering and fraudulent acts to the detriment of the institution; in the event of dubious or unusual practices in the light of past experience or knowledge of money laundering methods, the institution shall investigate these in the context of the current business relationship and individual transactions.

The Federal Financial Supervisory Authority may in individual cases issue orders to an institution which are appropriate and necessary for putting in place safeguards within the meaning of Sentence 3 No. 1 to 6.

(1a) Subsection 1 shall apply to groups of institutions, financial holding groups or financial conglomerates provided that the persons listed in Section 1 Subsection 2 Sentence 1 of the superordinated undertaking or of the superordinated financial conglomerate undertaking are responsible for the proper business organisation of the group of institutions, the financial holding group or the financial conglomerate. Section 10a Subsection 8 Sentences 1 and 2 as well as Subsection 9 Sentences 1 and 2 apply as appropriate to groups of institutions and financial holding groups, Section 10b Subsection 6 as well as Subsection 7 Sentences 1 and 2 apply as appropriate to financial conglomerates.

(2) The outsourcing to another undertaking of operational areas that are essential for conducting banking business or providing financial services must impair neither the orderliness of such business or services nor the managers' ability to manage and monitor them nor the Federal Financial Supervisory Authority's right to audit and ability to monitor them. In particular, the institution shall ensure by contractual means that it has the required powers to give instructions to the external service provider in question and shall include the outsourced areas in its internal monitoring procedures. The institution shall report its intention to outsource operational areas, as well as the realisation of its intention, to the Federal Financial Supervisory Authority and the Deutsche Bundesbank without delay.

(...)

### **Article 25c Internal safeguards**

(1) Notwithstanding the duties cited in section 25a (1) of this Act and section 9 (1) and (2) of the Money Laundering Act, institutions must – as part of their proper business organisation and appropriate risk management to prevent fraudulent activities – create and update, at their own expense, internal policies and adequate business and customer-related safeguards, and conduct checks.

(2) <sup>1</sup>Credit institutions must operate and update appropriate IT systems, which enable them to identify business relationships and individual transactions in payment operations that appear dubious or unusual in the light of knowledge of money laundering methods, terrorist financing and fraudulent activities to the detriment of institutions available publicly or within the credit institution. <sup>2</sup>Where such circumstances are identified, they must be investigated in the context of the current business relationship and individual transactions in order to be able to monitor and assess the risk involved in the relevant business relationships and transactions and, if necessary, examine whether there are grounds for suspicion. <sup>3</sup>The credit institutions may collect, process and use personal data insofar as this is necessary to fulfil this duty. <sup>4</sup>BaFin can lay down criteria which, if they are met, allow credit institutions to dispense with using the systems pursuant to sentence 1.

(...)

### **Section 25f Enhanced due diligence**

(1) <sup>1</sup>Over and above section 6 of the Money Laundering Act, institutions must comply with enhanced due diligence standards commensurate with a higher risk also in the settlement of payment transactions as part of business relationships with correspondent institutions domiciled in a non-EEA state. <sup>2</sup>Insofar as these business relationships do not concern the settlement of payment transactions, this is without prejudice to section 5 (2) number 1 of the Money Laundering Act. <sup>3</sup>Section 3 (4) sentence 2 of the Money Laundering Act shall apply *mutatis mutandis*.

(2) In the cases cited in subsection (1), institutions must

- 1 obtain sufficient publicly available information about the correspondent institution and its business and management structure in order to be able to understand fully, both before and during such a business relationship, the nature of the business operations conducted by the correspondent institution and assess its reputation and controls for combating money laundering and terrorist financing as well as the quality of its supervision,
- 2 lay down and document the respective responsibilities of both institutions with regard to compliance with the due diligence standards before establishing such a business relationship,

- 3 ensure that, before such a business relationship is established by an agent acting on the obligated party's behalf, he/she obtains the approval of his/her immediate superior or the next highest management level,
- 4 take measures to ensure that the correspondent institution does not establish or maintain a business relationship with a credit institution of which it is known that its accounts are used by a shell bank within the meaning of Article 3 (10) of Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJ EU L 309/15) as last amended by Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 (OJ EU L 319/1), and
- 5 take measures to ensure that the correspondent institution does not permit transactions via interim accounts.

(3) Notwithstanding section 3 (2) sentence 1 number 2 of the Money Laundering Act, the due diligence pursuant to section 3 (1) numbers 1 and 3 of the Money Laundering Act shall apply to obligated parties pursuant to section 2 (1) numbers 1 and 2 of the Money Laundering Act when accepting cash irrespective of any thresholds specified in the Money Laundering Act or in this Act, insofar as a customer's order in the context of money transmission services within the meaning of section 1 (1a) sentence 2 number 6 or foreign currency dealing within the meaning of section 1 (1a) sentence 2 number 7 is not settled via a customer account opened with the obligated party and the transaction with regard to foreign currency dealing involves a value of €2,500 or more.

(...)

### **Section 25g Group-wide compliance with due diligence standards**

<sup>1</sup>Institutions which are the superordinated enterprise of a group of institutions within the meaning of section 10a (1) or (2) or a financial holding group within the meaning of section 10a (3) or are the parent enterprise of a financial conglomerate within the meaning of section 1 (20) sentence 1 must develop group-wide internal safeguards pursuant to section 9 of the Money Laundering Act and section 25c (1) of this Act with regard to their branches and enterprises of which they have majority ownership and must ensure compliance with the due diligence standards pursuant to sections 3, 5 and 6 of the Money Laundering Act and sections 25d and 25f of this Act as well as the record-keeping obligation pursuant to section 8 of the Money Laundering Act, insofar as this is permissible under the laws of the state in which the branch or enterprise is domiciled. <sup>2</sup>The senior managers within the meaning of section 1 (2) sentence 1 shall be responsible for the proper fulfilment of the duties pursuant to sentence 1. <sup>3</sup>Insofar as the measures to be taken pursuant to sentence 1 are not permissible in a non-EEA state in which the enterprise is domiciled pursuant to the laws of that state, the superordinated enterprise or the parent enterprise must inform BaFin thereof promptly and take additional measures in order to effectively counter a higher risk of money laundering or terrorist financing. <sup>4</sup>If stricter obligations apply in the foreign state in which a branch or an enterprise is domiciled, these stricter obligations must be fulfilled there.

(...)

### **Article 29. Special Duties of the Auditor**

(1) When auditing the annual accounts or interim accounts, the auditor shall also examine the financial circumstances of the institution. When auditing the annual accounts, he shall ascertain in particular whether the institution has complied with the reporting requirements pursuant to Sections 10, 10b, 11, 12a, 13 to 13d and 14 Subsection 1, Sections 15, 24 and 24a, in each case also read in conjunction with a regulation in accordance with Section 24

Subsection 4 Sentence 1, in the case of Section 24a also read in conjunction with a regulation in accordance with Section 24a Subsection 5, and also whether the institution has satisfied the requirements pursuant to Sections 10 to 10b, 11, 12, 13 to 13d, 18 and 25a Subsection 1 Sentence 1 No. 1 to 3 and Subsection 2, in the case of Sections 13 to 13c and 14 Subsection 1 also read in conjunction with a regulation in accordance with Section 22. If unrealized reserves are included in the institution's liable capital, the auditor, when auditing the annual accounts, shall likewise examine whether Section 10 Subsections 4a to 4c was complied with when ascertaining those reserves. The findings shall be included in the auditor's report.

(2) The auditor shall likewise examine whether the institution has complied with its obligations under the Money Laundering Act (Geldwäschegesetz) as well as under Sections 24c, 25a Subsection 1 Sentence 1 No. 4 and 25b. In the case of institutions engaged in safe custody business he shall audit that business particularly carefully; this audit shall also cover compliance with Section 128 of the Stock Companies Act on disclosure requirements and Section 135 of the Stock Companies Act on the exercising of voting rights. The auditor shall report separately on the items mentioned in Sentence 1 and Sentence 2, respectively; Section 26 Subsection 1 Sentence 3 applies as appropriate.

(3) If, in the course of his audit, the auditor learns of facts which might warrant the qualification or withholding of the certificate of audit, jeopardise the existence of the institution or seriously impair its development, or which indicate that the managers have severely infringed the law, the articles of association or the partnership agreement, he shall report this without delay to the Federal Financial Supervisory Authority and the Deutsche Bundesbank. At the request of the Federal Financial Supervisory Authority or the Deutsche Bundesbank, the auditor shall elucidate the auditor's report to them, and communicate any other facts which have come to his attention in the course of the audit and which suggest that the business of the institution has not been conducted properly. The auditor shall not be held accountable for the accuracy of facts which he reports in good faith in accordance with this subsection.

(4) The Federal Ministry of Finance, in agreement with the Federal Ministry of Justice and after having consulted the Deutsche Bundesbank, may issue by way of regulation more detailed provisions on the object of the audit, the time at which it is carried out and the contents of auditor's reports, insofar as this is necessary for the performance of the functions of the Federal Financial Supervisory Authority, and especially in order to enable it to identify irregularities which may jeopardise the safety of the assets entrusted to the institution or which may impair the proper execution of banking business or provision of financial services, and to obtain consistent records for assessing the business conducted by institutions. It may delegate this authority by way of regulation to the Federal Financial Supervisory Authority.

(...)

### **Article 33. Refusing the License**

(1) The license shall be refused if

1. the resources needed for business operations, in particular adequate initial capital within the meaning of Section 10 Subsection 2a Sentence 1 No. 1 to 7, are not available in Germany; the initial capital which must be available is as follows:

a) in the case of investment brokers, contract brokers and portfolio managers who in

the course of providing financial services are not authorised to obtain ownership or possession of funds or securities of customers and who do not trade in financial instruments for their own account: an amount equivalent to at least fifty thousand Euro,

b) in the case of other financial services institutions which do not trade in financial instruments for their own account: an amount equivalent to at least one hundred and twenty-five thousand Euro,

c) in the case of financial services institutions which trade in financial instruments for their own account and in the case of securities trading banks: an amount equivalent to at least seven hundred and thirty thousand Euro,

d) in the case of deposit-taking credit institutions: an amount equivalent to at least five million Euro;

e) in the case of institutions which only conduct e-money business, an amount equivalent to at least one million Euro;

2. facts are known which suggest that an applicant or one of the persons specified in Section 1 Subsection 2 Sentence 1 is not trustworthy;

3. facts are known which warrant the assumption that the holder of an important participating interest or, in the case of a legal person, a legal representative or representative according to the articles of association, or, in the case of a partnership, a partner, is not trustworthy or for other reasons fails to satisfy the requirements to be set in the interests of the sound and prudent management of the institution; Section 2b Subsection 1a Sentence 1 No. 1, 2<sup>nd</sup> partial sentence applies accordingly;

4. facts are known which suggest that the proprietor or one of the persons specified in Section 1 Subsection 2 Sentence 1 does not have the professional qualifications necessary for managing the institution and if no other person has been designated as manager in accordance with Section 1 Subsection 2 Sentence 2 or 3;

4a. in the case of granting a license, the institution becomes a subsidiary of a financial holding company within the meaning of Section 1 Subsection 3a Sentence 1 or of a mixed financial holding company within the meaning of Section 1 Subsection 3a Sentence 2 and facts are known which warrant the assumption that a person within the meaning of Section 2c is not trustworthy or does not have the professional qualifications necessary for managing the financial holding company or the mixed financial holding company;

5. a credit institution or a financial services institution which, in the course of providing financial services, is authorised to obtain ownership or possession of funds or securities of customers or which according to a certificate from the Federal Financial Supervisory Authority pursuant to Section 4 Subsection 1 No. 2 of the Act Governing the Certification of Contracts for Private Pension Plans (Gesetz über die Zertifizierung von Altersvorsorgeverträgen) is authorised to offer contracts for private pension plans, does not have at least two managers who work for the institution not merely in an honorary capacity;

6. the institution has its head office outside Germany;

7. the institution is not prepared or not in a position to make the organizational arrangements necessary for the proper operation of the business for which it is seeking a license;

8. the applicant is the subsidiary of a foreign credit institution and the competent foreign supervisory authority for this credit institution has not given its consent to the establishment of the subsidiary.

An investment broker or a contract broker who in the course of providing financial services is not authorised to obtain ownership or possession of funds or securities of customers and who does not trade in financial instruments for his own account shall not be refused a license in accordance with Sentence 1 lit. a) if, instead of the initial capital, he can demonstrate that he has taken out appropriate insurance for the protection of customers.

(2) A prerequisite of the professional qualifications for managing an institution needed by the persons specified in Subsection 1 Sentence 1 No. 4 is that they have adequate theoretical and practical knowledge of the business concerned, as well as managerial experience. A person shall normally be assumed to have the professional qualifications necessary for managing an institution if he can demonstrate three years' managerial experience at an institution of comparable size and type of business.

(3) The Federal Financial Supervisory Authority may refuse to grant the license if facts are known which warrant the assumption that efficient supervision of the institution is impaired.

This is, in particular, the case if

1. the institution is associated with other individuals or undertakings into a corporate network or is closely linked to such a network which impairs effective supervision of the institution due to the structure of the cross-shareholdings or due to inadequate commercial transparency;

2. an effective supervision of the institution is impaired by the legal and administrative provisions of a non-EEA state applicable to such individuals or undertakings;

3. the institution is a subsidiary of an institution domiciled in a non-EEA state that is not effectively supervised in the state in which it has its domicile or head office or whose competent prudential agency is not willing to co-operate satisfactorily with the Federal Financial Supervisory Authority.

The Federal Financial Supervisory Authority may also refuse the license if the application, contrary to Section 32 Subsection 1 Sentence 2, does not contain sufficient information or documents.

(4) The license may not be refused for reasons other than those specified in Subsections 1 and 3.

(...)

#### **Article 44. Information from and Audits of Institutions, Ancillary Banking Services Enterprises, Financial Holding Companies and Undertakings Included in Supervision on a Consolidated Basis**

(1) An institution and the members of its governing bodies as well as of its employees shall upon request provide information on all business activities and submit documentation to the Federal Financial Supervisory Authority, to the persons and agencies the Federal Financial Supervisory Authority uses in performing its functions and to the Deutsche Bundesbank. The Federal Financial Supervisory Authority may perform audits at the institutions, even without a special cause, and may entrust the Deutsche Bundesbank with the task of carrying out such audits; this shall include undertakings to which an institution has outsourced major operational units within the meaning of Section 25a Subsection 2. The staff of the Federal Financial Supervisory Authority, the staff of the Deutsche Bundesbank and any other persons whom the Federal Financial Supervisory Authority uses to perform the audits may enter and inspect the institution's business premises for this purpose during customary office and business hours. The parties affected shall tolerate the measures taken under Sentences 2 and 3.

(2) A subordinated undertaking within the meaning of Section 10a Subsection 2 to 4, a financial holding company at the head of a financial holding group within the meaning of Section 10a Subsection 3 and a member of a governing body of such an undertaking shall upon request provide information and present



documentation to the Federal Financial Supervisory Authority, to the persons and agencies the Federal Financial Supervisory Authority uses in performing its functions and to the Deutsche Bundesbank to enable them to check the accuracy of the information or data supplied and which are required for supervision on a consolidated basis or which are to be supplied in accordance with a regulation pursuant to Section 25 Subsection 3 Sentence 1. The Federal Financial Supervisory Authority may perform audits at the institutions, even without a special cause, and entrust the Deutsche Bundesbank with the task of carrying out such audits; Subsection 1 Sentence 2, 2<sup>nd</sup> partial sentence applies as appropriate. The staff of the Federal Financial Supervisory Authority, of the Deutsche Bundesbank and the other persons the Federal Financial Supervisory Authority uses to perform the audits may enter and inspect the institution's business premises for this purpose during customary office and business hours. The parties affected shall tolerate the measures taken under Sentences 2 and 3. Sentences 1 to 4 shall apply as appropriate to a subsidiary not included in the consolidation and to a mixed company and its subsidiaries.

(3) Undertakings domiciled abroad which are included in the consolidation shall upon request allow the Federal Financial Supervisory Authority to carry out the audits permitted under this Act, in particular checks of the accuracy of the data supplied for the consolidation pursuant to Section 10a Subsections 6 and 7, Section 13b Subsection 3 and Section 25 Subsections 2 and 3, to the extent necessary to enable the Federal Financial Supervisory Authority to perform its functions and to the extent permissible under the laws of the other state. This shall also apply to subsidiaries domiciled abroad which are not included in the consolidation.

(3a) Subsection 2 Sentences 1 to 4 and Sentence 5, 1<sup>st</sup> alternative shall apply as appropriate to subordinated financial conglomerate undertakings within the meaning of Section 10b Subsection 3 Sentence 5 and to mixed financial holding companies as well as to members of the governing bodies of such undertakings. Subsection 3 applies as appropriate to subordinated financial conglomerate undertakings within the meaning of Section 10b Subsection 3 Sentence 5 domiciled abroad.

(4) The Federal Financial Supervisory Authority may send representatives to shareholders' meetings, general meetings or partners' meetings, as well as to meetings of the supervisory bodies of institutions organised in the form of a legal person. They may address these meetings. The parties affected shall tolerate the measures taken under Sentences 1 and 2.

(5) Institutions organised in the form of a legal person shall, at the request of the Federal Financial Supervisory Authority, convene the meetings specified in Subsection 4 Sentence 1, convene meetings of the administrative and supervisory bodies and announce subjects on which decisions are to be taken. The Federal Financial Supervisory Authority may send representatives to a meeting convened in accordance with Sentence 1. They may address the meeting. The parties affected shall tolerate the measures taken under Sentences 2 and 3. This is without prejudice to Subsection 4.

(6) The person required to provide information may refuse to answer questions the replies to which would expose him or one of the relatives specified in Section 383 Subsection 1 No. 1 to 3 of the Code of Civil Procedure (Zivilprozessordnung) to the risk of criminal prosecution or of proceedings under the Act on Administrative Offences (Gesetz über Ordnungswidrigkeiten).

(...)

#### **Article 60. Competent Administrative Authority**

The administrative authority (Verwaltungsbehörde) within the meaning of Section 36 Subsection 1 No. 1 of the Act on Administrative Offences is the Federal Financial Supervisory Authority.

(...)

## **8. Insurance Supervisory Act (*Versicherungsaufsichtsgesetz, VAG*)**

(...)

### **Article 80d**

#### Internal safeguards

(1) Without prejudice to the requirements laid down in Section 9 (1) and (2) of the Money Laundering Act, insurance companies as defined in Section 80c shall operate and update appropriate systems which enable them to recognize business relationships and individual transactions that should be regarded as suspicious or unusual on the basis of experience and knowledge generally and specifically available within the insurance company concerning methods of money laundering and terrorist financing. Where such activity is detected, it shall be investigated in the context of the ongoing business relationship and individual transactions in order to be able to monitor and assess the risk of these business relationships and transactions and to determine whether it constitutes suspicious activity. Where they use data processing systems for this purpose, insurance companies may gather, process and use personal data as needed to meet this requirement.

(2) Where an insurance company as defined in Section 80c maintains an internal audit unit, this unit shall check compliance with requirements to prevent money laundering and terrorist financing at least once a year. The report of audit results shall be presented to the senior management, the money laundering commissioner and the supervisory authority.

(3) Insurance companies as defined in Section 80c that are parent companies within an insurance holding company as defined in Section 104a (2) no. 4, of a mixed insurance holding company as defined in Section 104a (2) no. 5 or Section 104a no. 3 or of a financial conglomerate as defined in Section 104k no. 4 shall create internal safeguards in accordance with paragraph 1 and Section 9 of the Money Laundering Act for their branches and majority-owned subsidiaries which offer contracts as defined in Section 80c and ensure compliance with due diligence requirements referred to in Sections 3, 5 and 6 of the Money Laundering Act and Section 80e as well as the recording and retention requirements referred to in Section 8 of the Money Laundering Act, where permitted by the legislation of the country in which the branch or company is located. Senior management as defined in Section 7a (1) fourth sentence shall be responsible for ensuring that the requirements referred to in the first sentence are properly met. In cases where the legislation of the third country where the company is located does not permit application of the measures required under the first sentence, the higher-level company or parent company shall immediately inform the supervisory authority and take additional measures to effectively handle an enhanced risk of money laundering or terrorist financing. If stricter requirements apply in the third country in which the branch or company is located, these requirements shall be met in that country.

(...)

### **Article 80e**

#### Simplified due diligence

(1) Where the conditions laid down in Section 6 of the Money Laundering Act are not met, insurance companies as defined in Section 80c face a low risk of money laundering or terrorist financing in the following cases beyond those listed in Section 5 of the Money Laundering Act:

1. in the case of contracts as defined in Section 80c, where the amount of premiums to be paid over one year does not exceed EUR 1 000 or where a one-time premium paid does not exceed EUR 2 500;
2. in the case of insurance policies for pension insurance contracts which neither contain a buy-back clause nor can serve as security for a loan;
3. in the case of pension schemes, plans or comparable systems providing pension benefits for employees, where contributions are deducted from employee pay and beneficiaries are not allowed to transfer their rights to third parties;
4. in all other cases where the following conditions are met:
  - a) the contract is in writing;
  - b) the relevant transactions are carried out using the customer's account with a credit institution as defined in Section 1 (1) of the Banking Act (with the exception of those companies referred to in Section 2 (1) nos. 3 to 8 of the Banking Act), with a credit institution in another European Union Member State, with a domestic branch of a credit institution having its head office abroad, or with a credit institution located in a third country and subject to requirements equivalent to those in Directive 2005/60/EC;
  - c) the product or related transaction is not anonymous and allows for the timely application of Section 3 (2) no. 3 of the Money Laundering Act;
  - d) the contract sets a threshold as defined in the first sentence no. 1; and
  - e) the benefits from the contract or related transaction cannot be paid to third parties except in case of death, disability, exceeding a certain age limit or similar cases;
5. in the case of products or related transactions in which it is possible to invest in financial investments or claims such as insurance or other contingent claims where, in addition to the conditions laid down in no. 4
  - a) benefits from the product or transaction may be paid out only over the long term;
  - b) the product or transaction cannot be deposited as a security; and
  - c) no early payments can be made and no repurchase clauses can be claimed and the contract cannot be terminated before its date of maturity.

(2) Paragraph 1 shall not apply when the insurance company has information about a specific transaction or business relationship indicating a higher risk of money laundering or terrorist financing.

(...)

## **Article 80f**

### **Simplified identification**

(1) By way of derogation from Section 4 (3) of the Money Laundering Act, the requirement to identify policy holders laid down in Section 3 (1) no. 1 of the Money Laundering Act shall be deemed to have been met where the policy holder authorizes the insurance company as defined in Section 80c to withdraw the premiums via direct debit from the policy holder's account with a credit institution having its head office in a European Union Member State. If it is not possible to collect the premium from the account specified by the policy holder, the company shall identify the policy holder.

(2) Where an insurance policy contract concluded for an occupational pension on the basis of an employment contract or employment on the part of the policy holder contains an agreement that the premium is to be paid through the policy holder's account as specified in the contract, the requirement to

identify the policy holder shall be deemed to be met if the insurance company confirms that the premium is actually paid through the agreed account.

(3) By way of derogation from Section 4 (1) of the Money Laundering Act, an insurance company as defined in Section 80c may also verify the identity of the beneficiary designated in the insurance policy after the business relationship has been established. In this case, verification must be completed before benefits are paid out or before the beneficiary intends to claim his/her rights granted by the insurance policy.”

(...)

## Article 144

### Administrative offences in insurance business

(1) An administrative offence shall be deemed committed by any person who, as member of the management or supervisory board, as authorised agent (section 106 (3)) or as liquidator of an insurance undertaking

1. proposes or permits the distribution of profits determined in violation of statutory provisions or the approved operating plan relating to the establishment of provisions and reserves,
  - 1a. fails to appoint a claims representative in violation of section 7b (1) sentence 1,
2. violates a provision with respect to the investment of the guarantee assets, the other restricted assets or the segregated investment portfolio, the calculation, posting, custody or management of the mathematical provision or the *Deckungsstock* (sections 54 (2) sentence 1, also in conjunction with a regulation pursuant to subsection (3), section 54 (2) sentence 2, or section 54b (1) or (2) sentence 2, each also in conjunction with section 54c, sections 65 to 67, 77, 79, 110d (2) and (3)) or fails to issue or to correctly issue a certification in accordance with section 66 (6) sentence 6, also in conjunction with section 110d (2) and (3),
3. violates the approved operating plan with respect to the investment of cash,
4. carries on business not provided for in the approved operating plan or permits the carrying on of such business, or
5. violates a regulation pursuant to section 55a (1), also in conjunction with section 106 (2) sentence 4, to the extent that it refers to these provisions on administrative fines in relation to a certain offence.

The provisions concerning administrative fines pursuant to sentence 1

1. nos. 1, 3, and 4,
2. no. 2 to the extent that it relates to sections 54a, 66, 67, 77 or 79, and
3. no. 5 to the extent that it relates to section 55a (1)

shall also apply to pension funds pursuant to section 113.

(1a) An administrative offence is committed by any person who

1. intentionally or negligently violates a regulation in accordance with section 5 (6), section 12c, also in conjunction with section 110a (4) no. 2 or section 65 (1), to the extent that it refers to these provisions on administrative fines in relation to a certain offence,

2. intentionally or negligently fails to give notice in accordance with section 13b (1) or (4) sentence 1, section 13c (1), also in conjunction with subsection (4), section 13d nos. 1 to 6, 7, also in conjunction with section 110a (4) no. 2, or no. 8 or no. 9, section 13e (1) no. 1 or 2, subsection (2) sentence 1 or subsection (3) sentence 1, section 58 (2) sentence 1 or section 104 (1) sentence 1 and sentence 2 first half sentence, sentence 3 or 4 or subsection (3), each also in conjunction with a regulation pursuant to subsection (6) or section 121a (2), or does so incorrectly, incompletely or not within the prescribed period,
3. in violation of section 59 sentence 1, fails to submit or to submit copy of the auditor's report or fails to do so within the prescribed period,
4. intentionally or negligently violates an enforceable order in accordance with section 81b (1) sentence 2 or subsection (2) sentence 2, also in conjunction with subsection (4), or section 104 (1a) sentence 1 or 2, or subsection (2) sentence 2, or an enforceable requirement under section 8 (2) or section 120 (4),
5. intentionally or negligently violates an enforceable order in accordance with section 83 (1) sentence 1 no. 1, also in conjunction with section 83 (5a) or section 110a (4) no. 3 (a), or section 83 (1) sentence 1 no. 1a or subsection (2) sentence 1, each also in conjunction with section 110a (4) no. 3 (a),
6. in violation of section 83 (1) sentence 1 no. 5, also in conjunction with section 83 (5b) sentence 1 fails to grant the right to speak,
7. in violation of section 83 (1) sentence 1 no. 6, also in conjunction with section 83 (5b) sentence 1, fails to convene or announce meetings,
8. intentionally or negligently fails to tolerate a measure, in violation section 83 (1) sentence 2, subsection (3) sentence 3, or subsection (4) sentence 2, also in conjunction with section 83 (5a), or section 110a (4) no. 3 (a),
9. violates an enforceable order in accordance with section 87 (6) or section 121c (5), or
10. intentionally or negligently fails to communicate data, in violation of section 103a (2) in conjunction with a regulation pursuant to section 12c, or does so incorrectly, incompletely or not within the prescribed period, or
11. in violation of section 131 (1), fails to provide information, or to provide it correctly, completely or within the prescribed period, or fails to submit a document, or to submit it correctly, completely or within the prescribed period.

The provisions concerning administrative fines pursuant to sentence 1

1. no. 2, to the extent that it relates to section 104, and
2. number 4, to the extent that it relates to section 81b or 104,

shall also apply to reinsurance undertakings within the meaning of section 119 (1).

(2) The administrative offence is punishable by a fine of up to one hundred and fifty thousand euros in the cases referred to subsection (1) nos. 1 to 4 and subsection (1a) above, and by a fine of up to fifty thousand euros in the cases referred to in subsection (1) no. 5.

(...)

## **9. Investment Act (*Investmentgesetz, InvG*)**

(...)

## Article 25d

### Simplified due diligence

(2) Where the conditions laid down in Section 25f of this Act and in Section 6 of the Money Laundering are not met, institutions face a low risk of money laundering or terrorist financing in the following cases beyond those listed in Section 5 of the Money Laundering Act:

1. when issuing or managing electronic money as defined in Section 1 (14), as long as it is guaranteed that
  - a) if the data storage device cannot be recharged, the maximum amount stored in the device is no more than EUR 150; or
  - b) if the data storage device can be recharged, a limit of EUR 2 500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1 000 or more is redeemed in that same calendar year by the bearer as referred to in Section 22p (1);
2. subject to the second sentence when concluding
  - a) a contract for a state subsidized, fully funded private pension;
  - b) a contract for capital-forming investment, where the contract meets the conditions for state subsidies;
  - c) a loan contract, financial leasing contract or instalment sale transaction with a consumer (Sections 491, 500, 501 of the Civil Code (BGB));
  - d) a loan contract as part of a state subsidy programme carried out by a federal or state development bank, where the loan amount must be used for a designated purpose;
  - e) credit contract for instalment financing;
  - f) any other loan contract where the loan account serves the exclusive purpose of repaying the loan and the loan payments are withdrawn from the creditor's account with a credit institution as defined in Section 1 (1) (with the exception of those companies referred to in Section 2 (1) nos. 3 to 8), with a credit institution in another European Union Member State or with a domestic branch of a credit institution having its head office abroad;
  - g) a savings agreement; and
  - h) a leasing agreement;
3. subject to the second sentence in other cases where the following conditions are met:
  - a) the contract is in writing;
  - b) the relevant transactions are carried out using the customer's account with a credit institution as defined in Section 1 (1) (with the exception of those companies referred to in Section 2 (1) nos. 3 to 8), with a credit institution in another European Union Member State, with a domestic branch of a credit institution having its head office abroad, or with a credit institution located in a third country and subject to requirements equivalent to those in Directive 2005/60/EC;
  - c) the product or related transaction is not anonymous and allows for the timely application of Section 3 (2) first sentence no. 3 of the Money Laundering Act; and
  - d) the benefits from the contract or related transaction cannot be paid to third parties except in case of death, disability, exceeding a certain age limit or similar cases;
4. subject to the second sentence where products or related transactions in which it is possible to invest in financial investments or claims such as insurance or other contingent claims where in addition to the conditions laid down in no. 3
  - a) benefits from the product or transaction may be paid out only over the long term;
  - b) the product or transaction cannot be deposited as a security; and
  - c) no early payments can be made and no repurchase clauses can be claimed and the contract cannot be terminated before its date of maturity.

In the cases of the first sentence nos. 2 to 4, a low risk shall be deemed to exist only where the following threshold values are not exceeded:



1. for contracts referred to in the first sentence no. 2 ad a, b, d and f or for contracts referred to in the first sentence no. 3 and 4 a total of EUR 15 000 in payments;
2. for contracts referred to in the first sentence no. 2 ad c, e and h or for other contracts to finance goods or their use and where the property title is not transferred to the contracting party or user until all instalments have been paid, EUR 15 000 in payments per calendar year;
3. for savings agreements referred to in the first sentence no. 2 ad g with periodical payments of EUR 1 000 per calendar year or a one-time payment of EUR 2 500.

(2) Paragraph 1 shall not apply when the institutions or persons covered by this Act have information about a specific transaction or business relationship indicating a higher risk of money laundering or terrorist financing.

(...)

#### **10. Fiscal Code (*Abgabeordnung, AO*)**

(...)

#### **Article 154 – Authenticity of accounts**

(1) No one may under a false or fictitious name, for himself or for a third person, open an account or cause entries to be made in an account, give into safe custody or pledge valuables (money, securities, precious objects) or rent a safety deposit box.

(2) Whoever keeps accounts, holds valuables in safe custody or as a pledge or rents out safety deposit boxes shall make certain before doing so of the identity and the address of the authorised drawer and shall record the relevant particulars in suitable form, in the case of an account in the account itself. They shall ensure that they are able at all times to furnish information on the accounts or safety deposit boxes over which a person is authorised to dispose.

(3) In the event of contravention of subsection (1) above, credit balances, valuables and the contents of safety deposit boxes may be returned only with the consent of the tax office responsible for assessing the authorised drawer for income and corporation tax.

(...)

#### **11. Foreign Trade and Payments Act (*Aussenwirtschaftsgesetz, AWG*)**

(...)

#### **Article 2 Nature and Scope of Restrictions and Obligations to Act**

(1) To the extent that restrictions are permitted in this Act, it can be prescribed by statutory order that legal transactions and actions, in general or under certain conditions,

1. require authorisation or
2. are prohibited.

(2) The Federal Ministry of Economics and Technology can, in consensus with the Federal Foreign Office and the Federal Ministry of Finance, impose the necessary restrictions on legal transactions or actions in

the field of foreign trade and payments in order to avert a danger in individual cases to the objects of legal protection named in Section 7 (1). In the case of measures affecting the fields of capital and payment transactions or trade in foreign valuables and gold, agreement with the German Federal Bank shall also be made. The decree shall expire six months after its enactment, unless the restriction is imposed by means of a statutory order.

(3) Restrictions shall be limited in nature and scope to the extent necessary to achieve the objective stated in the licence. They shall be framed in a way hampering the freedom of economic activity as little as possible. Restrictions may affect existing agreements only if the desired objective is in substantial jeopardy.

(4) Restrictions shall be revoked as soon as and insofar as the reasons warranting their imposition no longer apply.

(5) Where independent obligations to act may be substantiated under this Act, paragraphs 3 and 4 above shall apply *mutatis mutandis*.

(...)

#### **Article 7 Protection of Security and of External Interests**

(1) Legal transactions and acts in foreign trade and payments may be restricted in order to

1. guarantee the vital security interests of the Federal Republic of Germany,
2. prevent a disturbance of the peaceful coexistence of nations or
3. prevent a major disruption of the foreign relations of the Federal Republic of Germany.

(2) According to paragraph 1 above, the following may be restricted in particular:

1. the export or transshipment of

a) weapons, ammunition and military equipment,

b) objects which are useful in the development, production or use of weapons, ammunition or military equipment, or

c) constructional drawings and other production documents for the objects cited in letters a and b above

in particular if the restriction serves the implementation of export control agreed in international co-operation;

2. the export of objects which are destined for the conduct of military actions;

3. the import of weapons, ammunition and military equipment;

4. legal transactions on industrial property rights, inventions, manufacturing processes and expertise relating to the goods and other objects listed under no. 1 above;

5. legal transactions on the purchase of resident companies which

- produce or develop war weapons and other military equipment, or
- produce cryptographic systems admitted for the transmission of governmental classified information by the Federal Office for Information Security Technology with the company's approval,

or legal transactions on the acquisition of shares in such companies, in order to guarantee the vital security interests of the Federal Republic of Germany; this applies in particular if the political and security interests of the Federal Republic of Germany or the military security precautions are jeopardized as a result of the purchase.

(3) Legal transactions and acts of German nationals in foreign economic territories, which are related to goods and other objects, as per paragraph 2 no. 1 above, including their development and production, may also be restricted under the objectives set out in paragraph 1, if the German national

1. holds an identification document of the Federal Republic of Germany or
2. would be obliged to possess an identity card if he had a residence in the area of application of this Act.

This applies in particular when the restriction serves to prevent the proliferation of goods and other objects, as per paragraph 2 no. 1 above, which was agreed in international co-operation.

(...)