REPORT

ON THE FIRST ROUND OF NATIONAL

MONEY LAUNDERING AND TERRORIST FINANCING

RISK ASSESSMENT

Public version

December 2016

The complete Report was approved by the Government of the Czech Republic on 9 January 2017 by a Government Resolution No. 5 of 9 January 2017.

Information contained in that Report is not intended for third parties, can only be used for the purpose of AML/CFT prevention and is subject to confidentiality pursuant to the AML Act, as amended.

CONTENTS

1.1 THE SCOPE OF SHARING

Some chapters of this Report contain classified information. The scope of sharing of classified information is provided below.

Chapter	Main author	Classified information: YES/NO	Scope of sharing of classified information
Glossary of Selected Terms and Abbreviations	FAU	NO	
Introduction	FAU	NO	
Methodology and Applied Procedures	FAU	NO	
Identification and Assessment of Threats and Measures for Their Mitigation	FAU + PoCR	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, obliged entities and their associations.
Tax Crime: Assessment	GFD	NO	
Credit Institutions: Banks, Cooperative Savings and Credit Unions and the CNB as Obliged Entities	FAU	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, obliged entities under Section 2 para. 1 letter a) of the AML Act and their associations.
Adminstrators of Investment Tools Market, a Central Securities Depository and Other Entities Maintaining Registers of Investment Instruments as Stipulated by Law	CNB	YES	Competent state authorities and CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, obliged entities stipulated in Section 2 para. 1 letters a) and b) points 1 to 4 of the AML Act and their associations.

Chapter	Main author	Classified information: YES/NO	Scope of sharing of classified information
Securities Traders	CNB	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, obliged entities stipulated in Section 2 para. 1 letters a) and b) points 1 to 4 of the AML Act and their associations.
Payment Institutions and Electronic Money Institutions	CNB	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, obliged entities stipulated in Section 2 para. 1 letters a) and b) point 5 of the AML Act and their associations.
Mobile Payment Service Providers	FAU	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, providers of mobile payment services, APMS, Donors Forum.
Insurance Industry	FAU	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, obliged entities stipulated in Section 2 para. 1 letters a) and b) point 8 of the AML Act and their associations.
Bureau de Change Sector	CNB	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, obliged entities stipulated in Section 2 para. 1 letters a) and b) point 10 of the AML Act and their associations.

Chapter	Main author	Classified information: YES/NO	Scope of sharing of classified information
Gambling Operators	FAU	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, obliged entities stipulated in Section 2 para. 1 letter c) of the AML Act and their associations.
Real Estate Trade	FAU	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, obliged entities stipulated in Section 2 para. 1 letters a) and d) of the AML Act and their associations.
Legal and Advisory Professions	FAU	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, obliged entities stipulated in Section 2 para. 1 letters a) and e) to g) of the AML Act and their associations and SRBs.
Trust and Company Service Providers	FAU + MoJ	YES	Competent state authorities and CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, obliged entities stipulated in Section 2 para. 1 letters h) and i) of the AML Act, as amended; (letter h) in the proposed Amendment of the AML Act) and their associations (trust and company service providers).
Financial Analytical Unit	FAU	NO	
Supervision by the FAU	FAU	NO	
Exemptions Under Section 34 of the AML Act	FAU	NO	
Supervision of the CNB	CNB	NO	

Chapter	Main author	Classified information: YES/NO	Scope of sharing of classified information
Supervision of the CTIA	CTIA	NO	
NOCA	NOCA	NO	
NKBT	NKBT	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence, all obliged entities under the AML Act.
The role of Customs Administration in Countering ML/TF Risks	CACR	NO	
Cross-Border Transport of Cash	CACR	NO	
The Role and Importance of GFD in Mitigating ML/TF Risks	GFD	NO	
Corruption as a Vulnerability Relevant for ML/TF Risks	MoI	NO	
Vulnerability of NPOs in Terms of ML/TF	MoI + FAU	NO	
Vulnerabilities in Prosecution of Crime	MoJ	NO	
Summary of Risks and Necessary Additional Measures	FAU	NO	
Summary of Most Important Conclusions	FAU	NO	
Number of STRs from 2010 to 2015	FAU	NO	
Threat Assessment	FAU	NO	
Assessment of Exposure to Threats	FAU	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU.

Chapter	Main author	Classified information: YES/NO	Scope of sharing of classified information
Assessment of Vulnerability Rate	FAU	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU.
Threats Analysis	FAU	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, all obliged entities and their associations.
Map of Vulnerabilities Identified at Supervision	FAU	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, all obliged entities and their associations.
Police Statistics	PoCR	NO	
Statistics of Prosecuted Criminal Activities	MoJ	NO	
Analysis of the UCCFC	PoCR	YES	Competent state authorities and the CNB, mandatory authorities in interinstitutional consultation, foreign authorities and international organizations with the same scope of competence as the FAU, all obliged entities and their associations.
Analysis of the Public Prosecutor's Office	PPO	NO	

1.2 GLOSSARY OF SELECTED TERMS AND ABREVIATIONS

4th AML Directive	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015
Act No. 240/2013 Coll.	Act No. 240/2013 Coll., on Management Companies and Investment Funds, as amended
Act No. 256/2004 Coll.	Act No. 256/2004 Coll., on the Capital Market Undertakings , as amended
Act No. 277/2013 Coll.	Act No. 277/2013 Coll., on Bureau de Change Activity, as amended
Act on Accounting	Act No. 563/1991 Coll., on Accounting, as amended
Act on Banks	Act No. 21/1992 Coll., on Banks, as amended
Act on Cash Payments Restriction	Act No. 254/2004 Coll., on Cash Payments Restriction, as amended
AML	Anti-money laundering
AML Act	Act No. 253/2008 Coll., on selected measures against legitimization of proceeds of crime and financing of terrorism, as amended
AML Decree	Decree No. 281/2008 Coll., on certain requirements for the system of internal principles, procedures and control measures against money laundering and terrorist financing, as amended
BO	Beneficial owner under Section 4 para. 4 of the AML Act
CACR	Customs Administraiton of the Czech Republic
Civil Code/CD	Act No. 89/2012 Coll., the Civil Code, as amended
CDD	Customer due diligence, as stipulated in Section 9 of the AML Act
CFT	Countering the financing of terrorism

CNB	The Czech National Bank
Country Codes	Two-letter country codes according to ISO 3166 standard, https://www.iso.org/obp/ui/#search
Criminal Code/CC	Act No. 40/2009 Coll., Criminal Code, as amended
Criminal Procedure Code	Act No. 141/1961 Coll., on Criminal Judicial Procedure, as amended
CSDP	Central Securities Depository Prague
CTIA	Czech Trande Inspection Authority
Decree No. 141/2011 Coll.	Decree No. 141/2011 Coll., on the pursuit of business of payment institutions, electronic money institutions, small-scale payment service providers and small-scale electronic money issuers, as amended
Decree No. 163/2014 Coll.	Decree No. 163/2014 Coll., on the performance of the activity of banks, credit unions and investment firms, as amended
Decree No. 315/2013 Coll.	Decree No. 315/2013 Coll., on bureau-de-change activity, as amended
EMI	Electronic Money Institution
FACR	Financial Administration of the Czech Republic
FATF	Financial Action Task Force, www.fatf-gafi.org
FAU	Financial Analytical Unit of the Ministry of Finance
FTF	Foreign terrorist fighter
Gambling Act	Act No. 186/2016 Coll., on Gambling
GFD	General Financial Directorate, superior authority for Tax Offices

LEAs	Law enforcement authorities
Lotteries Act	Act No. 202/1990 Coll., on Lotteries and Other Similar Games, as amended
LP	Legal Person
ML	Money laundering
MLRO	Money laundering reporting officer
Amended AML Act	Act No. 368/2016 Coll., amending Act No. 253/2008 Coll.
NADA	National Anti-drug Agency
NPO	Non-governmental non-profit organization
NOCA	National Organized Crime Agency of the Criminal Police and Investigation Service
NP	Natural Person
OCU	Organized Crime Unit of the Czech Police (now under NOCA)
Payment System Act	Act No. 284/2009 Coll., on the Payment System, as amended
PEP	Politically exposed under Section 4 para. 5 of the AML Act and in the Amendment of the AML Act
PPO	Public Prosecutor's Office
PPD	Protection of personal data
Public Registers Act	Act No. 304/2013 Coll., on Public Registers of Legal persons and Natural Persons, as amended
RBA	Risk based approach

RVNNO	Government Council for Non-Governmental Non-Profit Organizations
SPPO	Supreme Public Prosecutor’s Office
SSEMI	Small-Scale Electronic Money Issuer
STR	Suspicious Transaction Report as stipulated in Section 18 of the AML Act
TBML	Trade based money laundering
TF	Terrorist Financing
VAT	Value Added Tax
WMD	Weapons of mass destruction

1.3 INTRODUCTION

This Report summarizes main outcomes from the first round of the national money laundering and terrorist financing risk assessment.

Identification, understanding and assessment of risks are an integral part of effective risk management. On the national level and with respect to prevention and mitigation of ML/TF risks the aim is to formulate a national AML/CFT strategy. Risk assessment is a natural part of operation of either public or private subjects concerned. Nevertheless, one of the main goals of the national ML/TF risk assessment is to contribute to the national AML/CFT policy. The objective of a coherent risk based approach is a more effective allocation of financial but primarily human resources, both in public and private sector. Therefore, all subjects involved in the NRA aimed not only to collect data but foremost to formulate outcomes that would provide guidance. Providing guidance to and sharing of best practices with the private sector is one of the most important goals of this national risk assessment.

Regulators can manage risks either by legislative or non-legislative measures. However, national ML/TF risk assessment is primarily a process. This process consists of: exchange of ideas, sharing of information among stakeholders, formulation of objectives and submission of outcomes that facilitate implementation of practical measures based on provided guidance.

This is the first round of risk assessment in the Czech Republic. This process will be periodically repeated. The main methodology is set out in the *FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment*[1] and the obligation to conduct national risk assessment follows from the FATF Recommendation 1 and from the 4th AML Directive.

We express our appreciation to all those who took part on the first round of national ML/TF risk assessment: experts from competent state authorities and from private sector. To all of them we express our gratitude for information, materials, opinions and comments they had provided and last but not least for their time and openness to dialogue and sharing of ideas.

[1] http://www.fatf-gafi.org/publications/methodsandtrends/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

1.4 METHODOLOGY AND APPLIED PROCEDURES

The national ML/TF risk assessment procedures are guided by the FATF Methodology. The structure of the Report is based on the key risk functions: threats, vulnerabilities and consequences. Inseparable from these are mitigating measures.

This first round of RA focused on both money laundering and terrorist financing. In accordance with FATF R.1 risk of financing of proliferation of weapons of mass destruction was not a primary focus of the RA. Czech competent authorities decided to manage both ML and TF risks simultaneously, mainly because of their urgency and relevancy and also with respect to the follow-up procedures for their mitigation. Both ML and TF risks are very serious, although reasons are significantly different (e.g. high volume of property damage v. security, life and health threats). Authorities which took part in this NRA strove to evaluate risks from multiple angles and aimed to use all possible procedures (and available sources of information) in order to circumvent one-sided view. The multifaceted perspective enabled a cross-check of results of different procedures and approaches.

In accordance with FATF Methodology competent authorities understood risk as a function of: threat, vulnerability and consequences.

A ML/TF threat is:

- serious predicate offence, which causes significant damages and generates high amount of revenues, that perpetrators need to legalize;
- related money laundering techniques;
- terrorist financing techniques.

The threat analyses proved that the character of the predicate offence, to a large extent determines techniques of money laundering. In some cases the predicate offence is almost inseparable from the related (often not consecutive) money laundering technique, because some transactions, e.g. fictitious invoicing, are related to both tax evasion and legalization. The situation is similar regarding crimes committed abroad which are also conditional upon the related money laundering technique and eventually also the level of legalization of proceeds. This is reflected in the arrangement of the relevant part of the Report for the breakdown of typologies on predicate offences and on ML/TF techniques has emerged as a topic for an academic discussion.

When carrying out this national ML/TF risk assessment the competent authorities followed up on their continuous educational endeavour and strove to formulate a common opinion and to share information on risks, i.e. a form of a strategic feedback. For this reason the Chapter on threats includes primarily typologies in a form of sanitized cases accompanied by information on types of obliged entities exposed to such *modus operandi*; on most typical risk factors; and on most typical suspicious indicators. This information is also summarized in a table *Threat Analysis* annexed to this Report, which is available to all types of obliged entities. (Each type of obliged entity can find typologies it typically faces with most common risk factors and signs.) Due to the sensitive nature of information it contains, that Chapter is from a large part classified and is only available to obliged entities.

Following the characterization of typologies the next Chapter is on assessment of threats based on seriousness and dangerousness of their consequences and furthermore there is an outline of future development of threats. Assessment of consequences and their seriousness is not separated from the process of threat assessment. The Chapter closes with a description of vulnerabilities identified and assessed during threat analysis and with a description of measures for mitigation of vulnerabilities. Also in this case measures for mitigation are connected with risk assessment.

As outlined above, it was sought to feed the quantitative data with added value of expert opinions. In case of threats, it means, i.a., that there are on one side police and judicial criminal statistics and on the other side analysis and threat assessment based primarily on expert review of typologies, i.e. the crucial question of where and how criminal proceeds flow (i.e. as mentioned above: exposed types of obliged entities, significant risk factors and suspicious indicators). Expert assessment of threat consequences is a similar case, where level of seriousness and dangerousness could hardly be evaluated by quantitative data only.

Vulnerabilities are understood as vulnerable, weak points where identified threats can cause harm and which are susceptible to criminal abuse. In the assessment process vulnerabilities were viewed from different perspectives. Possible vulnerabilities were identified and analysed:

- With respect to insufficient legislature, those vulnerabilities were identified either during threat analysis, or during PESTEL analysis according to FATF Methodology or from sub-analysis of vulnerabilities of a certain type of obliged entity or field of services exposed to ML/TF risks;
- With respect to failure to comply with sufficient legislature, those vulnerabilities were identified during supervision (such data are presented in a *Map of Vulnerabilities Identified at Supervision* attached to this Report which includes all types of obliged entities as stipulated in the AML Act);
- With respect to inadequate compliance with AML/CFT prevention framework, however not identified during supervision. Such data are hard to quantify and compare, thus their evaluation is dependent on expert opinion and appraisal. Attention was focused on compliance in key elements of AML/CFT prevention such as customer due diligence, obligation to inform and report, irrespective of whether such inadequacies are reportable for the purpose of supervision (these data are presented in *Quantifiable Expert Appraisal of Vulnerabilities in the Private Sector* attached to this Report which includes all types of obliged entities as stipulated in the AML Act). This is a valuable source of information for formulation of a risk based approach of supervisory authorities;
- With respect to any other vulnerabilities identified during sub-analysis of vulnerabilities in each sector of respective obliged entity (the order of sub-analysis of vulnerabilities reflects the order of types of obliged entities in the AML Act).

Whereas the analysis and assessment of threats (including vulnerabilities stemming directly from threats) covers all types of obliged entities and other respective entities, the subjects of the last sub-analysis of vulnerabilities in the private sector were in this round of NRA: credit institutions, financial institutions such as investment market subjects and fund investment

subjects, payment services providers, insurance industry, bureaus-de-change, gambling operators, legal and advisory professions and trust and company services providers. Whereas sub-assessment of threats (and of vulnerabilities identified directly during the threat analysis) covered all types of obliged entities, sub-processes of segment vulnerabilities in the private sector covered most types of obliged entities. Selection of more deeply analysed market segments was conditional upon:

- The size of the segment;
- The level of exposure to ML/TF threats;
- Estimated amount of customers' assets managed by the segment;
- Number of STRs (e.g. relatively high or on the contrary low numbers);
- Importance for identification of threats;
- Seriousness and variability of threats it is exposed to; etc.

Chapters on respective segments of obliged entities provide a follow-up to our educational activities in a form of lists of specific risks factors (not only generally formulated suspicious indicators). These lists are tailored for the respective type of obliged entity and they include the widest range of situations arousing suspicion. Nevertheless, these lists are only indicative, because they obviously cannot cover all situations that obliged entities may face. Because these chapters or their parts contain sensitive information, the chapters or their respective parts are classified. They are available to the respective obliged entities. In most cases participation of experts from the private sector was sought, first in a form of an input to the sub-analysis and afterwards in a form of comments to the relevant part of the text. The respective description of a method and sources of information is listed in each chapter. Sub-analyses and sub-assessments of vulnerabilities also contain measures for mitigation of identified risks. Also in this case is a formulation of necessary mitigation measures a part of an ongoing process and not a separate plan.

In order to raise awareness, the Report also lists guidance for real estate agents, even though vulnerability of the real estate sector was not part of this round of NRA.

Consequences are inseparable from threats. In line with our effort to submit information directly useful for prevention of ML/TF risks, the seriousness of threat was considered from several key perspectives: seriousness of threats, frequency of threats and dangerousness of threats (dangerousness, damage to the public interest, organized character, difficulty to detect, etc.). Conclusions drawn are summarized in a chart *Assessment of Threats* attached to this Report and reflect both collected information and expert assessment.

Important element of the NRA is formulation of measures to mitigate identified and assessed risks. As stated above, formulation of measures is a part of risk management and is not dealt with separately in any other process or report. Specific measures are listed at the relevant sub-process from which they had stemmed. For a clear arrangement all measures are summarized in one chapter at the end of the Report. This summary does not contain any other information or description of risks other than those given in the respective chapters. Unnecessary repetition of previously drawn conclusions was avoided.

This national ML/TF risk assessment covers the whole AML/CFT framework. The scope of topics covers both assessment of prevention framework and assessment of effectiveness of prosecution of crimes and ranges so to say from customer due diligence to the conviction of perpetrators.

Discussions among competent authorities on the system of prosecution showed necessity of a detailed analysis of investigation and prosecution of crimes that represent ML/TF threats. Thus, attached to this Report are thorough analyses undertaken by the Supreme Public Prosecutor's Office and UCCFC CPIS of the Police of the CR.

In June 2016 FATF published newly revised Recommendation 8 on risk of abuse of NPOs for terrorist financing. Despite the fact that all substantive sub-processes had already been done or were being finalized, the NRA Coordinator decided to re-open the issue of vulnerability of NPOs and initiated an implementation of measures according to the new FATF R.8.

As stated above, one of the main goals of a national risk assessment is an effective allocation of resources and consequently to promote a risk based approach. For this reason the NRA focused on suspicious indicators, risk factors and types of obliged entities exposed to ML/TF. The same attention was paid to valid exceptions stipulated in the national or EU AML/CFT legislation. These exceptions were re-assessed to find out if they could be susceptible to abuse in connection with analysed threats. It is clear that monitoring of possible abuse of exceptions will remain of a particular interest. The risk assessment was in line with the principle *comply or explain*. For the exception to be acceptable the use of each exception must be justifiable and must be accompanied by appropriate additional measures mitigating residual risk. The process aimed at maintaining and enhancing effectiveness of the AML/CFT system, not at adding other exceptions.

The issue of financial inclusion is not a significant problem in the CR at the moment and the same applies to de-risking according to information from competent authorities. Customer due diligence is clearly set by valid legislation. Neither information from competent authorities nor findings from operational activity showed that the current practice is abused (or overused) and that transactions of certain groups of customers are pushed underground. However, with respect to the continuous migration crisis, this issue will be further monitored by competent authorities, because driving a segment of services or customers underground would seriously undermine the effectiveness of the AML/CFT prevention system.

The national risk assessment process involved to a different degree all competent public authorities. Apart from the Financial Analytical Unit other authorities involved were: Ministry of Finance, Ministry of Justice, Ministry of Interior, Ministry of Culture, Ministry of Foreign Affairs, selected units of the Police of the CR, the Supreme Public Prosecutor's Office, the Czech National Bank, supervisory authorities of the gambling industry, General Financial Directorate, Customs Authority, Government Council on Non-profit Non-governmental Organizations and Government Council on Co-ordination of Countering Corruption. During selected sub-processes experts from the Ministry of Regional Development and others were also consulted. Czech Trade Inspection Authority provided information from its supervisory activity. The competent authorities fulfil the following roles in the AML/CFT system: financial intelligence unit, law enforcement authorities, main AML/CFT prevention regulator, sector regulators, state supervisory authorities, central state authorities for issues relevant for the

system of AML/CFT prevention and prosecution, tax and customs authorities, selected specialized advisory bodies of the Government.

The FAU was a co-ordinator of the whole process. Sub-processes were carried out in smaller specialized teams consisting of experts from selected authorities based on their field of expertise. Teams were headed by leading experts responsible for the specific field. All other authorities could comment on the finalized part of the Report, i.e. experts from all competent authorities participating in the NRA had informally agreed on the draft of the whole Report. Involvement of each authority in sub-processes depended on its role in the AML/CFT system of prevention and prosecution. Each sub-process and the relevant chapter list the authority responsible for the analysed sector or problematics and the most important authorities involved. Furthermore, experts from the private sector provided input mainly into sub-analyses of vulnerabilities.

The weight of individual sources of information had been thoroughly assessed during each sub-process. Sources of information for NRA consist of: all information available to competent authorities and to the private sector consulted; and information from selected foreign open sources. Quality of information available had also been carefully judged; the question was if validity of information collected is relevant for the assessment or if in fact the current set of meta-data is only partially usable for the NRA. Dissemination of information that was discussed during sub-processes had been carefully considered due to the sensitive nature of such knowledge. In rare cases, discussion and dissemination of information in specialized teams had been considered satisfactory for the purposes of the NRA process. Many inter-agency meetings took place during the NRA and this Report reflects them. However, the Report does not contain any minutes from such meetings.

Some parts of the Report are classified with respect to the sensitivity of guidance provided. In such cases the classified part is highlighted in yellow. Scope of sharing is tailored for each topic or chapter or type of obliged entity and is specified in a table at the beginning of the Report.

It is necessary to emphasize again that the NRA is a process. This Report contains a summary of the most important findings of this process and thus, represents a form of a targeted dissemination of information, e.g. with relevant segments of the private sector or with decision-makers.

The submitted Report is on the first round of ML/TF NRA. It is thus necessary to adjust the frequency of the NRA. In accordance with Section 30 letter a) of the New AML Act, it is proposed to organize the second round of the NRA and submit a Report on it to the Government for discussion before 1 January 2021. With respect to future development of ML/TF risks certain parts of the NRA may be updated earlier.

2.1 IDENTIFICATION AND ASSESSMENT OF THREATS AND MEASURES FOR THEIR MITIGATION

The national ML/TF risk assessment process assumes identification and assessment of threats, of areas of vulnerability, of the impact of threats on vulnerable areas, assessment of current measures and drafting of new additional mitigating measures. This Chapter is primarily on threats as such. Nevertheless, some topics where it is especially relevant and where vulnerabilities directly result from threats, vulnerabilities and mitigating measures are outlined for identified risks (i.e., measures mitigating impact of threats on vulnerable areas[2]). The necessary measures mitigating risks (i.e. those identified directly at threat assessment) are dealt with at the end of this Chapter.

Primary objective of this Chapter is to raise awareness of and guidance for obliged entities stipulated by AML Act. Thus, it is not a reflection on already identified ML/TF threats in the Czech Republic that could have been drafted based on quantitative data[3], but this Chapter qualitatively assesses threats. The choice, characterization and assessment of threats were carried out as follows: initial wider list of threats (of both predicate criminal activity and ML/TF techniques) was compiled based on interviews with experts from the FAU and PCR. The list was then assessed by experts from the FAU and PCR and edited to reflect i) probability of identified threats (e.g. higher probability in case of frauds) and ii) seriousness (e.g. high seriousness of TF). A part of material including cases was provided by PCR. The FAU then added other cases and with respect to awareness raising and guidance provided exhaustive lists of i) types of obliged entities or other subjects, that could be exposed to described or similar risk and ii) possible risk factors and suspicious indicators relevant for the given typology. It is necessary to emphasize that the cases and typologies are a result of work of all stakeholders, not only of the FAU and PCR but also of obliged entities, which are indispensable for effective AML/CFT system.

Where relevant for awareness raising and guidance, topics (such as i.a. TF) are supplemented by cases from foreign open sources. In line with FATF Methodology a reasonable estimate of future trends of ML/TF threats was outlined[4]. This Chapter was provided for comments to all stakeholders: SPPO, GFD, CACR, MF, MoJ, MoI, CNB, CTIA and to some experts from the private sector. Non-highlighted text is public, however highlighted passages are classified and their sharing is specified at the beginning of this Report.

As stated above, ML/TF threats can be understood as an underlying criminal activity and as a ML/TF technique. Threats can be divided in this way; however, it is also true that the typology of predicate offence largely influences the technique of money laundering. Thus, where relevant the interconnection of both typologies is also described. This means that in case of certain predicate offences, the subsequent typical ML technique is identified and on the other hand the identification of certain ML/TF techniques is preceded by an outline of

[2] See FATF Metodology (risk: threat, vulnerability, consquences)
http://www.fatf-gafi.org/topics/methodsandtrends/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

[3] Quantitative data are provided in the annex to this National Risk Assessment Report.

[4] Such an expert estimate is based on open information, including from foreign sources.

predicate offence. Typologies are complemented by the following details: i) types of obliged entities typically exposed to certain technique or criminal activity, thus are able to detect such technique or crime (and avoid being exploited), or can participate in such criminal activity (by negligence or consciously); ii) risk factors (related to a customer, a service or a transaction) such as: scope of business, risk commodities, vulnerable legal forms; and iii) typical suspicious indicators used by obliged entities to detect suspicious transactions. The risk factors are partly stated in the text and further more listed at the end of each typology or at each specific case. On one hand, it was sought to list the widest range of risk indicators (they are not necessarily introduced in the specific case, but can be introduced in similar cases). On the other hand, it is necessary to emphasize that any such list cannot be exhaustive. The aim was to provide an initial guidance for ML/TF risk management of relevant obliged entities. In this context, the fact that e.g. risk commodities associated with certain typology can vary over time, although the *modus operandi* remains the same, should be born in mind.

The Prognosis of the Development

The prognosis of the development of crime is a process in which it is necessary to be aware of a number of factors influencing the commission of crime. First of all, it is necessary to be aware of the motives of the perpetrators, i.e. the reason why they commit the crime. In addition, it is necessary to analyse specific weaknesses of their subject of interest – of social values protected by criminal law (the object of a criminal offense) and the existing means by which the weak points can be "broken" and which the perpetrators have or may have at their disposal to commit the crime (weapons, information, money - in the case of bribery or financing – and IT equipment). This may be related to the creation of preventive measures to prevent or to minimize possible losses.

Taking into account the current global trend in developed countries, where the Czech Republic can undoubtedly be ranked, we see a great development in moving products (i.e. values) from the real world to the virtual world. Business corporations and other organizations, including the state, began to penetrate into the virtual world through retention of data concerning trading, records, etc. Whether it is communication among individual entities (state and private), dealing with different agendas, data retention, accounting, or using banking and insurance services on-line and online purchases of goods of all kinds. As more and more sensitive data and information are saved in electronic form and stored in computer technology, on servers, etc., the need for these data to be as secure as possible, not only against their loss but also against their misuse, grows.

Also, with the growing popularity of various social networks and the availability of Internet to the general public and the spread of so-called smart phones, the threat of attacks on such devices by perpetrators (using computer viruses, tracking, etc.) rises. Abuse of social networks to elicit personal data or access data to internet banking directly from users of such networks is also on the rise. Common users, either for their immaturity or ignorance, often fail to realize that, for example, the person they communicate with through social networks may not be the one that he/she poses to be, whether in terms of age and gender, not to mention the name.

The modern trend is also the creation of a completely new identity of people on the Internet, from the creation of an email, a bank account and profiles on social networks, to concluding contracts and carrying out other activities, etc. Perpetrators commit further criminal activity (especially fraud) under this completely new (and fictitious) identity. The use of so-called TOR networks is already a problem nowadays. TOR networks for the most part guarantee the anonymity of Internet users and it is very difficult to trace where the perpetrators access the network (also from what IP address), thus minimizing the possibility of detecting them.

Therefore, for each group of offenses, it is possible to predict that attacks using Internet and computing technologies will increase. As has already been mentioned, the subject of the perpetrators' interests – values – is shifting from real world to virtual. People are often introduced through social networks where they also spend most of their free time. It is thus tempting for perpetrators to create partially or completely fictitious identity. It is therefore clear that perpetrators, whether they commit general crime (fraud), economic crime (including fiscal crime) but also perpetrators of violent and moral criminality, will be more oriented to the internet environment, where user data, access to bank accounts, personal (and often

intimate) photographs (values, or approaches to values) are stored and there are possibilities to establish contacts with potential victims, etc.

The virtual world, the world of the future, will be an environment for the perpetrators to pick their victims (according to photos and information on social networks - for example, on the planned holiday of a person living in a luxury home) or to lure intimate pictures from children But it will be an environment where crime can also be committed – attacking interests protected by the law (phishing, extortion, fraudulent e-shops, publishing fake advertisement, accepting bribes, etc.). As a matter of principle, the independent functioning of the Internet also means that the cross-border crime will continue to increase in the future and that there is a need for very close cooperation among national competent authorities in sharing information and subsequent international cooperation.

Cash: a key risk vehicle and a consistent priority in risk management

Despite this undeniable trend, it is clear that in the next few years, cash transactions will continue to play a significant role, both in selected types of predicate offence and in laundering techniques and TF. In case of predicate offence, this phenomenon is particularly likely to occur where cash is direct proceeds of crime, as is typically the case for drug crime. However, cash transactions also apply to the laundering of proceeds of crime, which in itself does not generate cash, such as laundering of proceeds from fraud.

Specifically, in case of laundering proceeds of phishing, the typical *modus operandi* includes physical collection and transfer of cash or cash transport. In ML / TF techniques, cash transactions have an important role to play in situations where they interrupt the otherwise traceable chain (typically money transfers), or simply at the entrance to the system of regulated obliged entities (typically cash deposits on accounts, including ATM deposits, not only in the phase of placement of proceeds). This means that almost all perpetrators of economic crime use cash at some stage.

The main potentially vulnerable places with a high inherent risk and where these risks need to be further mitigated, include, in particular, cash deposits (including their structuring and including ATM deposits) and money transfers (including those intra-community, for which the Czech Republic is preparing a legal adjustment that would give the competent national authorities the authority to monitor and control (see the chapter on cash transfers).

Measures to mitigate identified risks

Each risk assessment must include the assessment of threats, vulnerabilities, possible impacts and the formulation of possible mitigation measures for the identified risks. Within the framework of the threat assessment process described above (i.e. both detected and those from foreign sources but also those outlined in the assessment of future developments), additional, or already existing, but particularly important risk mitigation measures were identified. Part of which falls under the AML / CFT prevention system and another part goes beyond the existing AML / CFT prevention system. These additional or the selected key measures are relevant in the context of the entire system of measures already in place so that the residual risk level of individual threats can be further reduced.

Supplementary measures beyond the AML/CFT prevention system

List of measures:

1/ Establishment of central register of accounts

2/ Obligation of legal persons to know their beneficial owner

3/ Register of data on beneficial owners of legal persons and trusts

4/ Register of Trust Funds

5/ Monitoring of intra-communitarian transports of cash

6/ Classification of Trust Funds among obliged entities

7/ Incorporation of some other operators of gambling among obliged entities

8/ Incorporation of virtual currency traders between obliged entities

9/ Possible involvement of insiders from the private sector

10/ Eventual involvement of insiders from the public sector

11/ Efficient TF prosecution

The following measures more detailed:

1/ Establishment of central register of accounts

The establishment of a central database of accounts kept by credit institutions for their customers, i.e. for natural or legal persons or other entities, is the subject of Government Resolution 168/2014 of 12 March 2014. The purpose of the central register of accounts is to enable competent public authorities to find out at a single location in a very short space of time at which credit institution a particular person has or had an account, the account of which it is or was the owner or the holder and, on the basis of that information, ask the relevant credit institution for details. Bypassing despatching of dozens of institutions, these will fail to manually retrieve and process negative information, minimize the risk of information leakage in sensitive cases and significantly increase the speed of access of competent authorities to information. Act No. 300/2016 Coll. will become fully effective on 1 January 2018.

2/ Obligation to know beneficial owner

In accordance with the requirements of the Fourth AML Directive, the New AML Act proposes to require all legal persons (and trustees of trust funds) to have up-to-date and accurate information about their beneficial owner, as well as an obligation to report that information to the appropriate register. The beneficial owner is the actual owner according to the AML Act (Section 4 para 4). The purpose of the amendment is to ensure, through the mandatory entries, the possibility of identifying a particular person or people who are the beneficial owners of the legal person (and similarly the trust fund) and, secondly, to identify the nature of the relationship and the extent and manner of shareholding. The register should therefore make it clear how the position of the beneficial owner is materially based. The legal persons

themselves (or the trustee of the trust fund) are responsible for the correctness of the data in the register. They must primarily have information about their beneficial owner.

3/ Register of data on beneficial owners of legal persons and trusts

Requirements to strengthen the transparency of legal persons and to establish a central register of beneficial owners of legal persons stem from the 4th AML Directive (Article 30). The Directive also requires similar measures, i.e. the register of beneficial owners in case of trusts – Article 31 under the Czech law. In the context of the above-mentioned requirements of the Directive, register of data on beneficial owners will be set out as a measure against the legalization of proceeds of crime and the financing of terrorism. Register should collect and store data to identify the beneficial owner and to provide information on the nature and extent of his holding or controlling influence in the legal person (or trust fund, respectively). For reasons of identification, it will be required to record those data that sufficiently specify a particular individual and potentially ensure his/her localization. Data on the name, date of birth, place of residence, or registered address and nationality are required in accordance with the requirements of the Directive. The extent of the recorded data on the beneficial owner of a trust is the same as of the beneficial owner of a legal person. Who is considered to be the beneficial owner of a trust will be based on the amended provision of Section 4 para 4 letter d) of the AML Act.

In addition to identification data, it is also necessary to record data specifying the relationship of the beneficial owner to the legal person (trust). The Directive requires not only information about who is the beneficial owner, but also why it is so in a particular case. Therefore, information will need to be gathered in the registry that specifies the basis on which a beneficial owner of a legal person has established its position. In essence, this information reveals the ownership structure of a legal person. The possible structure of the relationship (whether mediated) between the beneficial owner and the registered legal person (trust), including the specification of other links, should be apparent from the record.

Data on the beneficial owner will only be available to a limited number of entities (public authorities, obliged entities under the AML Act). A timely and unrestricted access will be set up for these entities, probably via an Internet application.

Requirements on transparency of legal persons stem from FATF R.24.

4/ Register of trust funds

Establishment of register of trust funds is the subject of an amendment to the Civil Code and other related laws submitted by Ministry of Justice (currently in the Chamber of Deputies). Specifically, register of trust funds will be regulated in Act No. 304/2013 Coll., on Public Registers of Legal and Natural Persons.

So far, trust funds have been registered only by individual public notaries. The only central register, exclusively for tax purposes, is register in the Automated Tax Information System.

Trust funds (or the trustee who is the person fulfilling duties of the tax entity) are obliged to register according to the tax rules and according to the relevant provisions of individual tax laws. The registration procedure is in the same as for other tax subjects - the trustee is

obliged to file an application for registration in cases specified by law, which includes a copy of the trust status and a prove of date of establishment of the trust and other documents proving the details given in the application form. However, this database is intended for tax purposes and is not public.

The proposal foresees the entrustment of registry to the registry courts. The register of trust funds should include not only the name and purpose of the fund, the date of its establishment and termination, the identification number, but also the information on the trustee, the founder, eventually the beneficiary, the person authorized to supervise the administration or the person exercising the decisive influence, data on the transfer of the plant, including the date of entry of recorded facts. It is also supposed to register similar legal arrangements under foreign law operating in the territory of the Czech Republic. The aim of the proposed legislation is to allow access to information to competent public authorities and to obliged entities subject to the AML Act, thereby increasing the transparency of trust funds and reducing the vulnerability of this legal arrangement. Fundamental data on the trust fund and the trustee should be accessible to the public, others not. All registered data will be accessible to the competent state authorities and obliged entities under the AML Act.

Transparency requirements for other legal arrangements (including trust funds) stem from FATF R.25.

5/ Monitoring of intra-communitarian transports of cash

Competent authorities are aware of identified threats. Preliminary work on the preparation of a legislative proposal on the introduction of control and monitoring of cash transfers within the Czech Republic and, possibly, across the Czech Republic with other Member States has already started on the initiative of the CACR. The aim of the intended system is to obtain a legitimate tool for the competent authorities to carry out this oversight and control. This includes in particular the possibility of requesting explanation and proof of origin of the transferred cash and possible detention and withdrawal of cash when suspected of illegal activity. The topic of cash transfers will be discussed in more detail in the relevant chapter.

6/ Classification of Trustees of Trust Funds and other trust service providers among obliged entities

Coverage of trustees or persons who provide services to another person under a trusteeship is subject to an amendment to the AML Act. Until now, only persons providing services under trust funds and similar legal arrangements under foreign law have been covered.

The inclusion of trust funds among the obliged entities in carrying out the defined activities follows, among others, from the FATF R.22 and R.23

7/ Incorporation of some other operators of gambling among obliged entities

Coverage of selected gambling operators, i.e. those who, having regard to the characteristics of the game, with regard to the characteristics of the related services provided, may be exposed to ML/TF threats, is also the subject of an amendment to the AML Act. The inclusion of gambling operators is based, inter alia, on the 4th AML Directive and the FATF Recommendations.

This Report will deal with specific assessment of the vulnerability of games of chance, depending on the characteristics of the game and the related services, in more detail in the section on the identification and evaluation of vulnerabilities.

8/ Incorporation of virtual currency traders between obliged entities

Virtual money is not recognized as an official currency. Nevertheless, services related to virtual money are already being carried out in the Czech Republic by various business entities, especially via the Internet and, even in brick-and-mortar shops. Such services include, for example, securing transfers of virtual currency (for goods or services and others), or the management of a virtual wallet or the exchange of virtual money for a fiat currency. The basic principles of AML/CFT prevention lie in the traceability of transactions and the principles of KYC, respectively CDD. These basic principles should be applied across the entire sector concerned, i.e. both in financial and in all non-financial entities, which can be exposed to ML/FT risks (so as to avoid potential vulnerabilities to ML/TF risks). To be added, ML/TF risks undoubtedly include concealment of the origin of assets that is threatens in the absence of CDD.

AML/CFT requirements for virtual currency service providers (as obliged entities) arise, inter alia, from the recently issued FATF document.[5]

A specific assessment of the vulnerability of this sector is in the relevant chapter.

9/ Measures to mitigate the risk of potential insider involvement in the private sector

Although such measures go beyond the scope of the AML/CFT prevention, it should be emphasized that the Criminal Code also considers the following: Firstly, Section 367 of the CC Non-obstruction of Criminal Offense also covers participation on a crime, legalization of proceeds of crime and terrorist attack (including the financing of terrorism). Secondly, the CC covers in § 217 also the negligent form of the crime of legalization.

Lastly, it should be added that according to the information available, the obliged entities have in place risk management systems related to internal fraud, especially with regard to their prevention and investigation. Part of AML/CFT training must also concern effective detection of potentially suspicious transactions and staff training so that, for example, a front office worker does not alert the customer to the inadequacy of some designations (e.g. money to help Syria) to avoid detection.

10/ Measures to mitigate the risk of eventual involvement of insiders from the public sector

The question of involvement of insiders from the public sphere in committing predicate offence is closely related to the transparent handling of public funds and the reduction of corruption risks in the performance of public administration. As part of the state's anti-corruption policy, a number of measures have recently been adopted, the common denominator being the interest in an open and transparent management of public budget and impartial civil service.

[5] http://www.fatf-gafi.org/topics/fatfrecommendations/documents/guidance-rba-virtual-currencies.html Minimal requirements for providers can be found on page 12.

These include the introduction of an obligation for the contracting authority to publish on its profile a public procurement contract (the price of which exceeded CZK 500 thousand), including all its amendments and additions, the amount of the price actually paid for the performance of the public contract. From 1 July 2016, the above measures should be complemented by the introduction of a register of contracts – an information system managed by the Ministry of the Interior. A number of contracts with commitments for public budgets will be recorded at one central location.

In addition, the Civil Service Act came into force, the main purpose of which is to de-politicize the state administration and the professionalism of civil servants. The Civil Service Act further links the new Code of Ethics for civil servants, according to which any corrupt conduct and biased decision-making by a civil servant is unacceptable.

11/ Efficient prosecution of terrorist financing

Terrorist financing according to a valid and effective legal regulation is punished as a criminal act of terrorist attack under Section 311 para 2 alinea 3 of the Criminal Code. This provision states that "the same [i.e., 5-15 years] will be punished, who such act [i.e. terrorist attack], terrorist, terrorist group or its member supports financially, materially or otherwise". Financial support means not only the direct provision of funds but also, in accordance with the provisions of Article 2 of the International Convention on the Suppression of the Financing of Terrorism, the unlawful and deliberate collection of funds with a view to their use or knowing that they are to be used, in whole or in part, to commit a terrorist attack.

This indirect collection of funds, according to foreign experience, occurs, for example, by camouflage for various church or humanitarian collections, foundations, etc., but may also involve other cooperation in obtaining funds for that purpose, or it may be contribution itself in awareness of what purpose the resources are to be used for. It is not decisive the origin of the funds intended to finance terrorism; it can be both legally and illegally obtained. As can also be seen from the above, financing of terrorism will also be the case if only part of the funds collected is used for terrorist activity or related support.

Last but not least, the promise and provision of reward to bereaved persons of perpetrators of suicide terrorist attacks is also becoming commonplace in the current world. Such behaviour should also be understood as the financing of terrorism. Material or other support for a terrorist, a terrorist group or a member of the group consists, for example, in the provision of space, meals, instruction, training and means of transport or other equipment. The so-called other means of support cannot be clearly defined, the most important criterion in assessing whether it is the support of terrorism is above all the sense of support provided and its intended use. The preparation of this crime is criminal as well as its attempt, as well as all forms of participation in the narrower sense (organizing, instructions, assistance).

It is true, that the present law is characterized by a high degree of generality, under which it is possible to categorize a whole range of various acts as fulfilling the characteristics of financial and other support for terrorism. By general regulation, the legislator usually leaves the judiciary a room for jurisprudence, while minimizing the need to respond by making amendments related to new types of socially harmful behaviour that arise in connection with development of crime.

Since the fight against terrorism is a topical issue and there is a need to effectively punish terrorism-related acts, it is proposed to amend the legislation in order to be more casuistic (which in general contributes to greater legal certainty). There is a proposal amending Act No. 40/2009 Coll., Criminal Code, as amended and other related laws that will be submitted to the inter-ministerial commentary procedure in February 2016 (the expected date of effect is 1 February 2017). This amendment will bring about fundamental changes in the legislation on the criminalization of terrorist financing, in particular a separate section on terrorist financing (Section 312b of the Criminal Code), which will also explicitly cover the collection of funds (directly and through another person).

Furthermore, a legal definition of a terrorist group, which reflects the requirements of Article 2 of Council Framework Decision 2002/475/JHA on Countering Terrorism, will be introduced. Further to the definition of terrorism, a new paragraph on participation in a terrorist group (Section 312 para 2 of the Criminal Code) should be introduced, which will lead to greater harmonization of the various provisions of the Criminal Code. The facts of the offense of a terrorist attack (Section 311 of the Criminal Code) will be supplemented to fully comply with the requirements of Article 7 of the Convention on the Physical Protection of Nuclear Material (27/2007 Coll. of Int. Treaties).

2.2 TAX CRIME AS AN UNDERLYING CRIMINAL ACTIVITY FOR MONEY LAUNDERING

Tax offenses can be considered as tax evasion (if a tax evasion is defined as a tax unaccounted for or accounted for but not granted for any reason) for which the facts are fulfilled within the meaning of the Criminal Code. However, this subset is from the social perspective very dangerous and harmful. The reason for committing this criminal activity is the property benefit to the detriment of the revenues of the state and the self-governing units. This property benefit must then be legalized. Legalization can take place in two ways: The first is abuse of the tax administration system, where a lower tax liability, such as a revenue reduction, will increase the taxpayer's disposable income or will enable him/her to obtain a comparative advantage in the market by lowering prices compare to competitors. The second is the legalization of proceeds of crime in the classical sense, such as by transferring funds intended to pay the tax from the company accounts using classical techniques, or recovering the funds spent on the payment of fictitious services or goods by means of non-mandatory cash records or hidden accounts.

It is worth mentioning once again that the value added tax present the highest risk, which is due to the nature of this tax, where the tax is the difference between the tax payable by the taxable transactions carried out by the payers and the right to deduct the tax on the received transactions. Value added tax arrears account for 60.9% of all tax arrears.

Tax crimes cannot be taken as an isolated crime. It can be clearly stated that in the large number of cases of corruption revealed the element of tax reduction was present. Failure to pay tax from fictitious invoices used to raise funds for corruption in awarding public contracts is a pleasant "bonus" for offenders. A company that has been awarded a public contract through a dedicated chain of subcontracting firms will reduce its profits and the obligation to pay VAT that would otherwise be due to a significantly overvalued contract price. These subcontracting companies led by the appointed statutory bodies will of course not fulfil their obligations and the funds received for fictitious subcontracts will pass through a covert way out of mandatory cash records or on hidden accounts of the organizers who use them to bribe public procurement and for their own benefit. Typically, fictitious advertising services, various forms of counselling and mediation or re-invoicing of services, materials, or merchandise already delivered are usually used for this purpose.

The perpetration of such a crime presupposes a high degree of organization and knowledge of both the tax and the financial system. In addition to this knowledge, it is necessary to locate and engage people who will be placed in the governing bodies of companies that will be in the position of Missing Trader (i.e., there, where the tax will not be paid in the supply chain). They are mostly people in a difficult life situation and therefore simply manageable. It is not difficult to acquire a company in itself, as there is a developed market in ready-made companies in the Czech Republic.

Furthermore, there is a need to develop a system of communication among fraudulent chain members that is difficult to trace and will protect the organizers from the inevitable investigation by the financial administration and the law enforcement bodies of Missing Traders. The communication must be bi-directional and must also allow the hidden transfer

of funds to pay the rewards to individuals in the chain. Communication is usually provided by people with experience with the LEA and able to follow conspiracy rules.

It is clear that groups of already established criminal organizations are able to provide such services to fraudsters to provide or manage fraud themselves. We cannot exclude the involvement of terrorist organizations for which VAT tax fraud can be a welcome source of funding.

Major risks from the point of view of the Financial Administration

- The value added tax system itself, where the tax liability is a tax difference that is burdened by the taxable payments made to payers and the right to deduct tax on the received transactions.
- Abuse of the simple establishment of legal persons in the Czech Republic and subsequently the developed market of readymade companies and accompanying services such as providing settlements, keeping accounts,
- The use of alternative payment methods, in particular non-banking payment service providers, complaining about the possible execution of funds from bank accounts in the event of non-payment of the tax.
- Deformation of the market environment where companies participating in fraudulent chains will be their suppliers are subject to reduced VAT are able to lower their prices or better trading conditions for their customers and thus also force other honest competitors to participate in such frauds.

Major measures taken by the Financial Administration to Mitigate the Risks

- Introducing the reverse charge mechanism for other groups of goods and services to minimize unjustified deductions.
- The introduction of control reports, which consist of the obligation of VAT payers every month to report to the financial administration on taxable transactions received and executed, which will allow rapid and effective control and detection of unauthorized deductions for transactions which the supplier has not admitted or failed to implement.
- Comprehensive scrutiny of new companies applying for VAT registration, so-called pre-registration checks. This measure is against the sale of readymade companies with already existing VAT registration. The intent of the financial administration is to ask for the registration to be the real owner who will carry out real economic activity through the company.
- Extending analytical activity, in particular by using the data from control reports so that the control activity can be streamlined by targeting precisely those entities that commit tax crimes.

3.1 IDENTIFICATION AND ASSESSMENT OF VULNERABILITIES IN THE PRIVATE SECTOR

3.1.1 CREDIT INSTITUTIONS: BANKS, CREDIT AND LOAN UNIONS AND THE CNB AS OBLIGED ENTITIES

Collaboration with financial institutions and, in particular, with banks and credit unions is crucial in terms of AML/CFT prevention. These institutions are exposed[6] to the increased ML/TF risks in terms of customer numbers, quantity and volume of processed transactions and are usually the most active in taking their own risk mitigation measures and reporting suspicious transactions. In preparation for the national risk assessment and AML amendment to the law, the FAU sent a joint questionnaire to all banks, foreign bank branches (45) and credit unions (11) that were listed on the CNB's list of regulated and registered entities (JERRS[7]) by December 2014.

The CNB had the opportunity to comment on the draft questionnaire before its distribution. The questionnaire was completed by 37 banks and branches of foreign banks, 10 credit unions and the CNB. The questionnaire had two parts: the first part is related to the national risk assessment and the second part is the basis for the preparation of the amendment to the AML Act and the RIA process (impact studies). Some respondents indicated completed questionnaires as "restricted" or "confidential". "Confidential". For this reason, part of this risk assessment with specific guiding information is not public.[8] The FAU subsequently gave the possibility to comment on this part of the report both to the CNB as supervisor and to individual respondents, the Czech Banking Association and the Association of Credit Unions and all state administration bodies involved in the ML/TF national risk assessment process.

The questionnaire survey[9] focused in particular on the following facts:

- How institutions categorize their customers in terms of money laundering and terrorist financing;
- Whether and how institutions categorize their products and services;
- How they detect suspicious transactions;
- To what extent the exceptions provided for by the AML Act are used;
- When they apply enhanced measures against ML/TF risks.

This part of the risk assessment is largely based on answers to the questions of the first part of the questionnaire, leaving most of the answers in the second part as part of the RIA project.

[6] I.e., the inherent risk is high here (assuming that risks are not mitigated, the sector would have a high vulnerability to ML/FT).
[7] https://apl.cnb.cz/apljerrsdad/JERRS.WEB07.INTRO_PAGE?p_lang=cz
[8] Also, with regard to the sensitivity of the information, we do not give a specific source, even though the submitted evaluation is in principle a compilation and, exceptionally, it is based on the findings of the questionnaire survey and the resources of the FAU.
[9] In line with FATF standards, we assume that the entire national risk assessment process will be repeated periodically/as needed.

Overall, the following can be summarized[10]:

- Credit institutions operating in the Czech Republic show very good awareness of AML/CFT prevention;
- In this context, they usually have well managed risk management: ML/TF risks are identified, evaluated and mitigation measures are adopted, all within the risk-based approach;
- Higher risk products or customers are compensated for by enhanced controls (frequency, depth);
- At the time of writing, some institutions were already working on a risk analysis; some were in the process of preparation;
- In this group of respondents, there are differences in the level of responses or risk management, but it cannot be said that these differences would be depend on the type of institution (banks vs. foreign bank branches, banks versus credit unions, entities with a large number of customers versus those with a small number etc.);
- In some cases it seems that ML/TF risks mix with other risks;
- Although the approaches differ, it can be concluded from the answers that a large number of institutions comply with the *comply or explain* rule;
- In the case of a minority of institutions for which it is unambiguous to answer that question, therefore - and at this stage of preparation so far only by this way - the FAU recommends revising the risk management system, in particular in the light of the *comply or explain* rule (e.g. with regard to the application of exceptions, risk mitigation and justification in cases where institutions consider some situations to be less risky).

The individual risk assessment of each institution must include a clear risk categorization, as it will only help the institution to allocate the necessary reasonable resources to mitigate specific risk categories. Such an analysis (its entire process) must be properly documented, updated and relevant components should be properly communicated, particularly within the institution, i.e. to the lowest level of work positions. Determining a specific measure of CDD (identification, customer due diligence and ongoing monitoring of transactions - frequency and depth) must be based on individual risk assessment of the institution and customer risk profiles. In this context, we recommend to the institutions to pay attention to the FATF Guidance for a Risk-Based Approach the Banking Sector.[11]

It should also be noted that no specific risk assessment below can be generalized simply because the specific solutions and approaches are based on individual risk analysis (risk based approach). Therefore, some approaches to risk assessment must necessarily be different depending on the composition and size of the customer portfolio, the products and services provided, etc. It follows that the specific indication of the level of risk must be based on a justification that can be based on the knowledge of a specific institution's risk. The generalizations presented here cannot be applied without limitation to each institution,

[10] Please note that the questionnaire survey did not evaluate individual responses and approaches in terms of their accuracy.

[11] http://www.fatf-gafi.org/topics/fatfrecommendations/documents/risk-based-approach-banking-sector.html

process, product, etc. However, at this stage, one of our objectives is to provide a first set of procedures and experiences as a guideline for institutions that process their own risk assessment. In the context of applying the principle of *comply or explain,* it should be stressed that those situations considered by institutions to be without risk must be adequately justified in their risk analysis and justification must be documented.

In the following breakdown, we distinguish who is the risk-taker, i.e. whether the risk taker is the customer, product or distribution channel, etc. At the same time, the resulting risk must take into account, in particular, the risk-taker, who presents higher risk. In the event that an AML non-risk customer uses AML risk product / service (or risk distribution channel, or has a risk legal form, etc.), institutions must take this risk into account in their procedures. Transferring the risk (such as a risk product) to the customer is one of the options that institutions can handle by taking into account the increased risk (associated with the risk product).

3.1.5.1 MOBILE PAYMENT SERVICE PROVIDERS

This chapter draws from the following sources:

- Report on “Risk Assessment of Mobile Payment Services in the Czech Republic with regard to Legalization of Proceeds of Crime and Terrorist Financing according to current FATF Recommendations” published by the Association of Providers of Mobile Services, processed by SVS consult s.r.o.[12], hereinafter “APMS Report”;
- Supplementary consultations with Association of Mobile Service Providers Association of Providers of Mobile Services (hereinafter “APMS”);
- Consultations with selected mobile operators;
- Supplementary consultations with Donors Forum;
- Relevant FATF documents;
- Information from the FAU.

The FAU also enabled competent authorities and obliged entities to provide input to this part of the Report.

Mobile operators can provide mobile payment services. In this case and provided that the conditions of the Payment System Act are fulfilled: the payment service providers are of a small extent and hence also obliged entities pursuant to Section 2 para 1 letter b) point 5 of the AML Act. Small-scale payment service providers are defined in the Payment System Act. So-called aggregators (mobile payment intermediaries), who are also payment service providers and therefore also obliged entities under the AML Act, are also involved in the provision of these services (their processing and settlement).

Mobile operators providing mobile payment services are permitted to perform payment transactions by an electronic communications service provider if the payer's consent to execute a payment transaction is given through an electronic communication device (pursuant to Section 3 para 1 letter g) of the Payment System Act), which is also stated in the List of Regulated and Registered Entities of the CNB (JERRS[13]). Mobile payment services provided by mobile operators are:

- Premium SMS: payments for goods and services through specially charged SMS (e.g., fare, parking, ringtone, mobile application, media voting, etc.);
- DMS: sending gifts to selected NPO accounts through specially charged SMS (always CZK 30); The Donors' Forum (hereinafter “DF”) implements the DMS project, i.e., donor SMS. DMS are intended for all non-profit organizations in the Czech Republic that meet specified parameters. Any non-profit organization that meets the conditions, especially transparent management (has public annual and financial reports for the past two years), publishes in advance the purpose for which people will

[12] APMS: Risk Assessment of Mobile Payment Services in the Czech Republic with Regard to Legalization of Proceeds of Crime and Terrorist Financing According to Current FATF Recommendations, author SVS consult s.r.o., Prague 2014.

[13] Single register of regulated and registered entities: https://apl.cnb.cz/apljerrsdad/JERRS.WEB07.INTRO_PAGE?p_lang=cz

contribute through DMS, etc. can participate in the donor SMS project. Furthermore, in compliance with the Act on Public Collections has an active collection (authorized by regional authorities or the City Hall of Prague). For more details: http://www.darcovskasms.cz/pro-neziskove-organizace/registrace-organizace-a-dms-projektu.html. In addition, the DMS Council, which is an independent body in which individual mobile operators, the DF and non-profit organizations are represented, is also involved in each project. The DF brings together leading Czech foundations and funds (about seventy members), some of whom use DMS, others not. The scope of the project is therefore wider and does not only serve its members. A complete list of all entities involved in DMS is public: http://www.darcovskasms.cz/seznam-projektu/prehled-projektu.html. A list of projects completed in the last six months is also available on the Web: http://www.darcovskasms.cz/seznam-projektu/uzavrene-projekty.html The DMS service is provided by the DF in cooperation with APMS and mobile operators, which are associated with the Association of Mobile Network Operators (APMS). Only those foundations or endowment funds that joins the Ethical Principles of the DF and meet the membership requirements of individual Associations at the DF (such as transparency, compliance with voluntary standards, Quality Grade of the DF for Foundations and Funds, Regular Disclosure of audited annual and financial reports, allocation of funds through open grant calls to at least five entities per year, or at minimum of CZK 250 thousand, etc.). However, the use of donor SMS services is not conditional on DF membership - other legal forms of NPOs than foundations or funds may also be involved and it is crucial that they meet the quality requirements (http://www.darcovskasms.cz/pro-neziskove-organizace/registrace-organizace-a-dms-projektu.html). In addition to NPOs, some donor organizations have the opportunity to raise money through donor SMS - especially zoos. However, they also have to meet the set parameters. The organization and project review is carried out by the DF upon entry into the system and on a continuous basis. Any NPO that receives funding from DMS is also subject to scrutiny by regional authorities or the City Hall Of Prague (because they are implementers of public collections, which are authorized and controlled by the relevant regional authority or municipality);

- M-payments: payment in an e-shop via an internet payment gateway, connection to a SIM card is either by a mobile data connection or in the case of another data connection in the form of a password from the SMS;
- Audiotex: a call service on specially charged phone numbers starting with numbers 90 with different audio content (counselling, dating, vistas, erotic services, access to websites, etc.)[14]

These services are charged as a deduction from the credit on a prepaid SIM card or by counting to the invoiced amount for a post-paid card.

In addition, there are options for making payments from a bank account or from a credit card through a mobile phone connection. These are outgoing payments for goods or services when the mobile connection only works as a communications payment solution. Despite the used name, this is not a mobile payment and the given payment method is therefore beyond the scope of this chapter.

[14] APMS, 2014, pp. 15-24

The payment service agreement between the customer and the mobile operator is either in writing or the agreement is closed by activating the SIM card or via an activation SMS. Customers are aware of the fact that if they make available to a third party the SIM card, PIN or passwords the customer is responsible for making any transactions as if they had done them themselves (until they notify loss, theft, abuse).

The operator is responsible for a payment from a customer to a payment aggregator. In the case of merchant of goods or premium service providers, the aggregator is responsible for the payment. The mobile payment service provider is also an obliged entity under the AML Act.[15] Thus, the mobile operator may not bind the aggregator contractually to fulfil obligations arising from the AML Act, since the requirements to ensure the sharing and storage of information, including informational and reporting obligations, apply to both types of providers.

[15] The list of mobile payment providers is available on websites operated by the APMS http://www.platmobilem.cz/pro-verejnost/seznam-zprostredkovatelu-mobilnich-plateb ; Prices for those services can also be found on this site.

3.1.6 INSURANCE INDUSTRY

Insurance companies, reinsurance companies, insurance intermediaries and independent insurance liquidators, with the exception of the insurance intermediaries with which the insurance company is liable for the damage caused by their activities, are subject to the AML Act in the performance of activities related to the life insurance.

In February 2015, the FAU sent a joint questionnaire to select entities providing life-insurance that were listed on the CNB's list of Regulated and Registered Entities (JERRS[16]) as part of the preparation of the NRA and AML Amendment. The questionnaire survey[17] focused in particular on the following facts:

- How do subjects categorize their customers in terms of ML/TF;
- Whether and how entities categorize products and services provided;
- How do they detect suspicious transactions;
- To what extent they use alternative ways of identification;
- In which cases they apply reinforced measures against ML/FT risks.

The questionnaires were completed by the following entities: 15 insurance companies, 2 associations of intermediaries, 2 independent liquidators.[18] This chapter draws mainly from the information of the FAU, from the information provided by obliged entities during the consultation and from the relevant FATF documents[19]. The draft of this text was also provided for comments and supplements to the MoF, the CNB, the MoI, the MoJ, LEAs, Czech Association of Insurance Companies, the Union of Financial Intermediation and Consultancy and the Association of Financial Intermediaries and Financial Advisors of the Czech Republic and all individual respondents.

Based on the consultation below are partial or general findings:[20]

- the sector is well aware of AML/CFT prevention;
- institutions also have a well-managed risk management: ML/TF risk are identified, evaluated and measures are taken to mitigate them, all within the RBA;
- higher risk products or customers are balanced by enhanced CDD;
- even in this group of respondents there are differences in the level of responses or in risk management;

[16] https://apl.cnb.cz/apljerrsdad/JERRS.WEB07.INTRO_PAGE?p_lang=cz

[17] This part of RA is largely based on respones to question from the first part of the questionair and most of the responses from the second part have been left aside, because they are part of RIA project.

[18] One addressed association of intermediaries, two intermediaries, one independent liqudator, three insurance companies and one reinsurance company have not responded to this questionair survey. Two entities stated that they do not provide life insurance.

[19] For example, http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfguidanceontherisk-basedapproachforthelifeinsurancesector.html

[20] Upozorňujeme, že cílem dotazníkového průzkumu nebylo hodnotit jednotlivé odpovědi a přístupy z hlediska jejich správnosti.

In some cases, ML/TF risks appear to be mixed with other risks, such as the risk of insurance fraud.

RBA allows entities to effectively implement AML/CFT preventive measures while appropriately allocating resources. (In addition, there are also minimum legal requirements that have to be fulfilled regardless of the RBA.) Outputs from individual RA, including the determination and assessment of risk factors, are crucial to RBA. Overvaluation of some risks could lead to over-allocation of resources, while underestimating risks would create vulnerabilities. Each individual RA must take into account both the probability of risk and its seriousness on the basis of all the available information. (For example, the TF risk is unlikely but very serious.) Reasonably applied risk mitigation measures then reduce the risk to an acceptable level. The individual RA of each institution must include a clear categorization of the risk types of customers, products and transactions, as it will help to apply reasonable assortments of measures to mitigate particular risk categories. Such an analysis (and its entire process) must be properly documented, updated and relevant components should be properly communicated, particularly within the institution, i.e., to the lowest level of employment and equally, to the extent appropriate and practicable, among the insurance company, its intermediaries and or liquidators. Determining a specific measure of CDD (identification, CDD and ongoing monitoring of transactions – frequency and depth) must be based on individual RA of the institution and customer risk profile.

Each of these types of obliged entities is involved in the transaction at a different stage. Among other things, it follows from the following:

- Insurance intermediaries play a key role in assembling the customer's risk profile, respectively. When identifying information within the customer identification and CDD, which is a prerequisite for the initial risk profile of the customer (in addition, in this respect it cannot be ignored cases where the intermediary knows his customer in relation to more arranged products, or not only in the field of insurance). For this reason, targeted training of intermediaries is particularly important, especially with regard to customer-related risk factors and the detection of potentially suspect customer behaviours in insurance policies (including follow-up measures leading to eventual submission of OPOs) as well as setting up effective communication mechanisms between the intermediary and the insurance company.
- Insurance intermediaries for which an insurance company is liable for damage caused by their activities are not an obliged entity under the AML Act but act on behalf of the insurance company and must be bound by its internal rules. There is no need to add that here too, the communication between intermediaries and the insurance company plays a big role.
- On the other hand, insurance companies are those who, on the basis of all available information (i.e. not only from contract management), determine the factors necessary to categorize customers and products, as well as signs to detect potentially suspicious transactions; they also determine an appropriate measures to mitigate identified risks (depth and frequency of CDD, including transaction reviews and follow-up measures, including STRs submissions). It should be added that the ultimate responsibility for identification performed pursuant to Section 11 para 5 of the AML Act is borne by the insurance company.

- Independent liquidators usually deal with damage from property and liability insurance, but if they provide life insurance services, AML/CFT obligations also apply to them.

Last but not least, it should be noted that no single RA below can be generalized simply because the specific solutions and approaches are based on individual risk analysis. Some approaches to RA must therefore necessarily vary depending on the composition and size of the customer portfolio, the products and services provided, etc. It follows that a specific indication of the degree of risk must be based on a justification that is based on the institution's knowledge of risks. However, at this stage, one of our goals is to provide a first set of procedures and experiences as a guideline for institutions that process their own RA. In the context of the application of the principle of comply or explain, it must be emphasized that for those situations considered by the institutions to be low-risk, such an assessment must be sufficiently substantiated in its risk analysis and documented.

In the following breakdown, we distinguish who poses a risk, i.e. whether it is the customer who bears the risk, or the product or the distribution channel; or signs of suspicious transaction, etc. At the same time, the resulting RA must take into account, in particular, the higher risk. In the case that an AML low-risk customer uses AML high-risk product/service (or a risk distribution channel or has a risk legal form, etc.), the institution must take this risk into account in its procedures. Transferring a risk (e.g. of a risk product) to the customer is one of the ways for institutions to ensure that increased risk (associated with the risk product) is taken into account.

3.1.8 GAMBLING OPERATORS

The term "gambling" means a game in which a bet is placed by a better and whose outcome depends on accident or previously unknown events.[21] The term "gambling operator" is a collective name for persons authorized to operate gambling in accordance with the relevant legislation.[22] Other, illegally operated gambling or even unfair games are not subject to the national ML/TF RA process. Gambling operators are obliged entities according to the 4th AML Directive, with casino game operators being obliged entities already according to the current AML Act (see below).[23] These are the so-called designated non-financial businesses and professions (DNFBPs).

This chapter deals collectively with all gambling games where any degree of risk of ML/TF has been considered. The chapter draws on information from the FAU and the State Supervision of Betting Games and Lotteries of the MF and other authorities concerned, from the relevant FATF reports[24], from the consultation of the MF with representatives of the obliged entities, or their associations through a questionnaire survey, or from publicly available sources. The questionnaire survey was held in February and March 2016 and the Ministry of Finance received answers from twenty operators: nineteen operators and one association of operators. The drafting of this part of the report was sent for comments to representatives of all stakeholders in the NRA of ML/TF. The FAU also subsequently allowed all respondents to comment on the draft of this chapter.

[21] Other, illegally operated gambling or even unfair games are not the subject of a national ML/TF risk assessment process. Such conduct is criminalized as an unauthorized operation of a lottery and similar betting game in accordance with the provisions of Sections 252 or 213 of the Criminal Code (Practise of Unfair Games and Wagers). This crime was not included among ML/TF threats.

[22] Currently Act No. 202/1990 Coll. is in force. At the same time, however, within the framework of a comprehensive recodification of the gambling sector, the Ministry of Finance prepared a new Act No. 186/2016 Coll., On gambling. The New Gambling Act will become effective as of 1 January 2017. From that date, the Customs Administration of the Czech Republic will have a new competence to supervise compliance with certain obligations laid down by the AML Act. The primary task of the Customs Administration of the Czech Republic in 2016 was also to ensure a smooth transition of the new comptence of the state supervision in the field of gambling from the Financial Administration of the Czech Republic in order to ensure effective supervision in the field of legal or illegal gambling operation as of 1.1.2017.

[23] http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatf-recommendations.html

[24] In particular:
http://www.fatf-gafi.org/publications/methodsandtrends/documents/vulnerabilitiesofcasinosandgamingsector.html

3.1.10 LEGAL AND ADVISORY PROFESSIONS

The term "legal and advisory professions" is a summary designation of a part of obliged entities as recommended by the FATF. These are the so-called designated non-financial businesses and professions (DNFBPs), which include "lawyers, public notaries, other independent legal professions and charted accountants"[25]. In accordance with the AML Act, auditors, tax advisers, charted accountants, court bailiffs performing statutory activities and public notaries and lawyers in performing statutory activities.

This chapter concerns all activities of all given professions.[26] For these obliged entities a special regime in the sense of Sections 26, 27, 37 and 40 of the AML Act applies. These provisions also imply a special status of selected professional chambers. The interpretation of the law will not be dealt with at this point. Activities of trust and company service providers according to Section 2 para 1 letter h) of the AML Act will be discussed in another chapter. This chapter draws on the FAU's information, from the relevant FATF report[27], from the FAU consultation in the form of a questionnaire survey with the representatives of obliged entities or with professional chambers, or from publicly available sources, such as the ISA 2403 International Auditing Standard or the Methodology Tool "Course of Action for Auditors in Countering Money Laundering and Terrorist Financing".[28]

As a response to the questionnaire survey, which was held in February 2015, the FAU received answers from the following bodies: Czech Bar Association, Chamber of Executors, Chamber of Auditors of the Czech Republic, Chamber of Charted Accountants of the Czech Republic, Chamber of Tax Advisors of the Czech Republic, Association of Accountants/ Chamber of Charted Accountants, Notary Chamber of the Czech Republic and one accounting company. Two addressed accounting companies did not join the survey. The draft of this part of the Report also was provided for comments to representatives of LEAs, MF, MoI and MoJ. The FAU also subsequently allowed all respondents to comment on the proposal.

[25] http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatf-recommendations.html

[26] It would be redundant to repeat, e.g., that activities related to the processing of wages are not carried out by public notaries. On the other hand, if, for example, a tax advisors provide other legal persons with their seat, as well as other related services, they are also an obliged entity in the course of carrying out this activity, NB high risk.

[27] http://www.fatf-gafi.org/topics/methodsandtrends/documents/mltf-vulnerabilities-legal-professionals.html

[28] Methodology Tool "Course of Action for Auditors in Countering Money Laundering and Terrorist Financing", http://www.kacr.cz/metodicka-podpora

3.1.11 TRUST AND COMPANY SERVICE PROVIDERS

Legal persons and other legal arrangements may be misused in some schemes of money laundering or terrorist financing (or other serious predicate offence). For this reason, providers of listed services for companies are included among the obliged entities under the AML Act. As trust funds are a new institution in the Czech legal system, the AML Act has so far covered only service providers for trusts and similar arrangements under foreign law. The amendment to the AML Act, in accordance with FATF Recommendations[29], includes trust and similar arrangements service providers under the Czech law.

Given the fact that the set of situations, or types of services that may be misused for committing crime, in principle coincides with both types of obliged entities, we have decided to outline the possible risks in one summary chapter.

The list of services listed below includes situations where obliged entities are exposed to ML/FT risks and can therefore manage (identify, assess and mitigate) the risks. For this purpose, in addition to the implementation of the basic measures under the AML/CFT prevention (see below), the lists of risk factors and suspicious indicators may also be used.

In addition, the risks associated with the legal form of trusts should also be considered. That is why at this point we include a more detailed description of the legal form.

Characteristics of the trust fund and its legal regulations

Since the effectiveness of the new Civil Code, a new institute - the Trust – has been introduced. This institute was inspired by foreign trusts, which is widely spread in common law. It is a popular legal form of asset management, which can take a wide variety of forms. However, basically the trust is a legal relationship between persons from whom one manages the assets so that the other person benefits from it.

With respect to the trust, the Civil Code distinguishes three basic entities - the founder, the beneficiary and the trustee. The trust is created by setting aside assets in the ownership of the founder and entrusting the assets to the fund manager for a particular purpose and the trustee pledges to hold and manage the assets. The creation of a trust results in separate and independent ownership of the allocated assets and the trustee is obliged to take over these assets and its administration (Section 1448 para 1 and 2 of Act No. 89/2012 Coll., the Commercial Code - hereinafter “Commercial Code” or “CmC”).

The trust is not a legal person. The purpose of the trust is to set aside assets that become so-called lying assets without an owner managed in favour of a beneficiary or a determined purpose. Ownership rights to assets in the trust are exercised by the trustee in his/her own name on the trust's account. However, the assets in the trust are neither the property of the trustee, nor the founder, nor the beneficiary (Section 1448 para 3 of the Commercial Code). The purpose of the trust may be either publicly beneficial or private (Section 1449 para 1 of the CmC).

[29] FATF Recommendations, R.22 a R.23, www.fatf-gafi.org

We can therefore define the trust as an entity without legal personality that allows for the creation of separate and independent ownership of assets entrusted to fulfil a particular purpose, whether public or private, with the assets deposited in the trust ceasing to be in the ownership of the trust's founder without them becoming the ownership of anyone else. At the same time, under the current legislation, the trust is not, in principle, subject to statutory oversight.

A trust is established either by contract or by acquisition in case of death (Section 1448 para 1 CmC). In the case of establishment of a trust in case of death, the trust is created as of the death of the testator; otherwise it is created only after a commission to administer the trust was accepted by a trustee. Each trust must have a statute issued by the founder and in the form of a public document. The Statute according to the current legal regulation contains at least the designation of the trust, the identification of the assets that constitute the trust at its creation, the definition of the purpose of the trust, conditions for performance from the trust, the indication of the duration of the trust, if the term is not stated, it is considered established for an indefinite period and, should there be a performance to a beneficiary, the beneficiary has to be determined or the manner in which it would be determined must be by defined (Section 1452 CmC).

Unless the Statute of a trust specifies otherwise, its founder appoints and recalls the trustee (Section 1455 para 1 CmC). Any legally competent person may be a trust. A legal person may be a trustee if the law so provides (Section 1453 of the CmC). At present it is only Act No. 240/2013 Coll. This Act, in the provision of Section 11, allows in certain circumstances, that an investment company becomes a trustee. The trustee may also be the founder of the trust or the beneficiary of the trust. In such a case, however, the trust must have another trustee, who is a third person (Section 1454 of the CmC). The trustee is entrusted with complete management of the assets in the trust. For this reason, the trustee is recorded in a public list or in another record as the owner of the assets in the trust with the note "Trustee" (Section 1456 CmC). The performance of a trustee is subject to requirements imposed on the management of foreign property (Section 1400 et seq. CmC) and the founder and the beneficiary, or any other person specified by the statute or by law (Section 1463 of the CmC), supervise the execution of his/her authorization.

The founder has the right to appoint a beneficiary and to determine the performance from the trust, unless the status of the trust determines otherwise. If the founder does not use this right, the trustee appoints a beneficiary and determines the performance from the trust. In the case of a trust set up for private purposes, the trustee may exercise this right if the statute determines the persons from whom the beneficiary can be appointed (Section 1457 para 1 and para 2 of the CmC). The right of the beneficiary for the performance from the trust is established under the conditions stipulated by the statute (Section 1459 CmC).

A trust can be used in practice e.g., to solve problems related to the management of large family assets and their intergenerational transition, as the trust allows for a broader subsequent control and intervention by the founder than in the case of donation or standard inheritances. In addition, a trust can be established, e.g., in order to achieve a specific business plan of several entities, instead of an association of entrepreneurs in a business consortium or to support a sports club, etc.

Risks associated with trust

Since a trust is not a legal person and therefore does not have a legal personality, it is not yet the subject of public registers. Under current legislation, statuses of trusts are recorded only by individual public notaries.[30] This prevents public authorities to supervise trusts and consequently, they have no idea of the number of existing and newly created trusts. The establishment of a trust in its current form allows the founder and beneficiaries of trusts to remain anonymous. Although a founder is detectable from a trust statute, a prerequisite for tracing the statute is the identification of a public notary, who wrote it and keeps it. It would usually be an extremely difficult task. and due to the factual unavailability of the statue, the founder and the beneficiary remain hidden both for general public and public authorities. An undesirable consequence of this is the vulnerability of a trust as a tool for legalization of proceeds of crime and possibly terrorist financing.

Perpetrators may use a trust as a tool for handling assets without their link to this legal arrangement being traceable, which significantly reduces the key tool of AML/CFT prevention which is the traceability of assets. However, attention should be drawn to an amendment to the Penal Code, implemented by Act No. 86/2015 Coll., amending Act No. 279/2003 Coll., On Securing Assets and Property in Criminal Proceedings and on Amending Certain Acts, as amended and other related laws. This amendment has made it clear that the object of seizure may also be an asset which is part of a trust, where, in the case where an asset of a trust is seized or an asset of a trust is to be seized, a trustee have a status of a participant in the criminal proceedings.

The absence of a sufficiently transparent central record of trusts and hence data on their establishment and on a trustee and a founder pose a problem in terms of the protection of the legitimate interests of third parties, in particular creditors. There is a limitation on the usefulness of institutes designed to protect third parties (e.g., relative inefficiency). In this context, it must be added that the risk of non-transparency of trust funds is already being legislated. At present an amendment to the Civil Code and other related laws (currently in the Chamber of Deputies) put forward an establishment of a trust register in which complex data on trusts will be recorded.

In accordance with the requirement of Article 31 of the 4th AML Directive the Ministry of Justice prepared a proposal on an establishment of a record of trusts and their BOs as an amendment to the Act on Public Registers of Legal and Natural Persons. The proposal is part of a government proposal amending Act No. 89/2012 Coll., the Civil Code and other related Acts and is currently being circulated as Press No. 642 in the Chamber of Deputies (1st reading was held on 4 May, 2016). The evidence should include both trusts established under the Czech law and foreign trusts under the law of another state operating in the territory of the Czech Republic.

Trusts represent a great vulnerability because they can be used for almost any purpose, are not subject to any supervision by public authorities and the possibility to be informed in order to protect interests of third parties is complicated by the inherent characteristics of this legal arrangement.

[30] Nevertheless, the Financial Authority for the City of Prague, which keeps records of trusts for tax purposes, currently registeres already 162 trusts (May 2016).

3.2 THE ROLE STATE AUTHORITIES AND THE CNB IN MITIGATION OF ML/TF RISKS

3.2.1 FINANCIAL ANALYTICAL UNIT

The Financial Analytical Unit is the coordinator of the national risk assessment process and is also the umbrella for the system of AML/CFT prevention in the Czech Republic.

In this system, it fulfils important tasks. The primary task is the function of an FIU. This means that as a national unit the FAU collects, analyses and shares information on suspicious transactions. For the purpose of analysing suspicions of money laundering, terrorist financing and related predicate offence also has significant powers to request relevant information from both the private and the public sector. The result of the work of qualified personnel is the high quality of the produced criminal notifications to the law enforcement authorities, i.e., the Police of the Czech Republic, in particular and other outputs provided to the Financial Administration and the Customs Administration. The high standard of information (including detailed financial data and information obtained from CDD) is also provided to foreign financial intelligence units as part of international co-operation.

Financial intelligence units may be of different types: administrative, police or otherwise. The fact that the FAU is an administrative unit brings key benefits for its activities. Of the most important, it is the fact that it can quickly and efficiently require important information from obliged entities necessary to analyse suspicious transactions.

On the other hand, the FAU provides obliged entities with specific feedback on individual STRs, as well as strategic feedback in the form of model cases, typologies and other related information such as risk factors and suspicious indicators. This awareness-raising activity and the resulting information are crucial to individual risk assessments that must also be carried out by individual obliged entities. Continuous contact with the private sector represents a high added value that the FAU brings to the AML/CFT prevention system in the Czech Republic.

Another important area under the responsibility of the FAU is the AML/CFT legislation. In other countries, this task is often based in a Ministry of Finance or supervisory authorities, etc. The fact that the main AML/CFT regulator is the Financial Intelligence Unit brings a great work commitments and unquestionable synergies in the implementation of the risk-based approach based on expert knowledge from our analytical work. In addition, in the field of legislation, the FAU provides interpretative statements to obliged entities and other state authorities. Frequently asked questions are published on the FAU website and its staff provides numerous training in AML/CFT prevention or application of international sanctions (see below).

The FAU is also a supervisory body in the field of AML/CFT prevention. In supervising certain types of obliged entities, it cooperates with other supervisory authorities, such as the CNB, the CTIA and authorities for the supervision of gambling. This imaginative solution, where the supervisory activity in the Czech Republic is a part of the financial intelligence unit, brings considerable advantages in the application of the risk-oriented approach to supervision.

There is no need to emphasize the importance of effective cooperation between the Analytical and Supervision Departments.

Another important area under the responsibility of the FAU is national coordination of the implementation of international sanctions. Also, in this field, the FAU carries out numerous tasks that stem from the relevant legislation on targeted restrictive measures. We also provide numerous interpretative opinions and training on this topic.

The amount and scope of the FAU's tasks is binding and places great demands on its internal communication, but it also provides ample space for synergies that are key to the risk-oriented approach.

As of 1 January 2017, the amendment to the AML Act establishes the Financial Analytical Bureau as a separate administrative office, which acts as a financial intelligence unit. The Office will have formal autonomy for the exercise of its powers on behalf of the State. Although it will not have separate legal personality, its material, technical and personal resources will be separate from the Ministry.

3.2.1.1 SUPERVISION BY THE FAU

The Supervision Department of the FAU performs, within the scope of its competence, tasks in the exercise of administrative supervision and administrative penalties based on the fulfilment of obligations arising from special legal regulations for ML and TF and from special legal regulations governing the application of international sanctions.

The supervisory activities of the Supervision Department are based on a Control Plan drawn up in accordance with the relevant provisions of the Control Procedure Code. Creation of the Control Plan is regulated by predetermined procedures and principles applied with respect to conditions relevant to the FAU. It is drawn up as a list of obliged entities to be supervised by the Supervision Department in a given year. It is based mainly on knowledge gained from the Department's control activities, analysis of financial market developments, activities of other departments of the FAU and, last but not least, the analysis of trends in ML/TF risks, which is a prerequisite for an effective application of the RBA. In order to eliminate possible duplication and possible overloading of obliged entities, it is modified with respect to control plans of other authorities supervising this area. The control plan is also characterized by a certain degree of flexibility with respect to external stimuli received or immediate negative findings related to activities of obliged entities.

The large variation in the type of obliged entities and, in particular, their large number in relation to the number of persons performing supervision, requires new ways and procedures for improving supervision of compliance with AML/CFT legislation and of the application of international sanctions. Implementation of an effective control tool in the form of mystery shoping, joint inspections with other supervisors, optimization of the time of inspections and close cooperation, in particular with the FAU's Analytical Department, has produced very positive results and improved supervisory activities of the Supervision Department. The number of inspections of obliged entities has increased, types of controlled entities have expanded (covering virtually all their spectrum) and the related number of breaches of legal obligations by obliged entities has increased. Streamlining and accelerating of performance of supervision has undoubtedly been facilitated by the adoption of a Methodological Instruction on Inspection. Its consistent application also affects obliged entities which are now under less burden of the supervisory process. The Supervision Department has also focused on prevention. A template for the System of Internal Policies and a template for designation of a MLRO is available on the FAU's website. These templates serve obliged entities as a tool in fulfilling some of their administrative duties under the AML Act.

The correctness and especially the effectiveness of established procedures for performance of administrative supervision and penalties are also confirmed by data from annual statistics.

Activity	2011	2012	2013	2014	2015
Number of supervisions	8	7	14	27	51
Number of administrative proceedings	3	13	19	18	35
Amount of imposed fines (CZK)	1.150.000	630.000	3.011.000	1.815.000	2.470.000

3.2.1.2 AUTHORIZATION OF EXEMPTIONS UNDER SECTION 34 OF THE AML ACT

The FAU decides on exceptions under Section 34 of the AML Act. These exceptions apply in the vast majority to bureaus de change operated as a "secondary activity", especially in hotels and spas; in limited number also, e.g., to electronic money issuers or carriers to operate electronic ticketing. Granting an exception is possible only if it is practically ruled out to misuse it for ML or TF. This means that as of the date when the decision to grant the exemption has come into effect, the relevant obliged entity ceases to be an obliged entity.

The specific conditions under which an exemption may be granted are transposed from the Commission Directive 2006/70/EC of 1 August 2006 (hereinafter referred to as the 'Implementing Directive'). Conditions are set cumulatively, which clearly reduces misuse for ML/FT:

a) The activity carried out is only an ancillary activity which is related to the principal activity of the applicant and the exemption cannot be granted to an entrepreneur who would remain an obliged entity under another provision of the AML law.

b) The limit for the annual turnover of this activity is a maximum of 5% of the total annual turnover of the obliged entity. According to the requirements of the Implementing Directive, this limit should be reasonably low and be set at national level. The FAU may set it up on an ad hoc basis, taking into account the possible structure of the applicants. If this limit was exceeded at the time of the exemption, this would be a reason to withdraw the exemption.

c) The Implementing Directive also sets a limit for a single transaction so that it does not exceed EUR 1,000 per individual customer. The AML Act also provides for a reasonable period of thirty consecutive days in which even a sum of multiple low transactions with the same customer the amount cannot be exceeded. Therefore, the entity which is granted the exemption must be able to control the counting of lower amounts and must document relevant measures to comply with this obligation in the application form.

The FAU may, at its discretion, grant this exemption only for a specified period of time and may also specify additional obligations to the extent of the obligations of obliged entities under the AML Act that it deems necessary to prevent abuse of the exemption for ML or TF.

Pursuant to Section 34 para 6 of the AML Act, after the granting of the exemption, a possible inspection by a relevant supervisory authority, i.e. by the CNB or by the FAU itself, is possible. In which case the following options will apply:

1. Prior to an on-site visit, a competent supervisory authority may, in cases where exceptions may apply, inquire whether an exemption has been granted to an entity. The record is kept by the FAU. The FAU will electronically notify the requesting authority of the text of the valid decision. During the inspection, it is also possible to check the fulfilment of all obligations under the AML Act from its effective date (1 September, 2008) until the decision to grant the exemption comes into effect.

2. After the exemption has been granted, the entity is not an obliged entity under the AML Act; therefore it is not obliged to have a system of internal policies, to carry out training, etc., unless certain obligation is retained in the decision to grant an exemption (see above). However, the entity remains obliged to report suspicious transaction it encounters it. This is in fact an extension of the reporting obligation that also results from criminal law. However, it cannot be deduced that employees should actively search suspicious transactions or be trained to do so. Similarly, such obligations cannot be enforced under criminal law. However, it follows from the law (and i.a. from the justification of the decision) that granting of an exemption is without prejudice to provisions of Sections 18 and 24 of the AML Act.
3. Once the exemption has been granted, the supervision will focus on compliance with conditions of the exemption and may lead, if appropriate, to its revocation, which would be decided by the FAU based on and initiative of a supervisory authority. Such supervision will therefore focus in particular on the following:

    a. Whether the relevant activity concerned by the exemption remains "secondary" and whether the obliged entity does not perform any other activity that would assign it among obliged entities under Section 2 of the AML Act;

    b. Whether the turnover ratios of secondary and core business according to Section 34 para 2 letter b) of the AML Act are still fulfilled; This fact does not need to be checked for the period considered to be decisive for the exemption decision but shall apply for each subsequent closed accounting period. In addition, the entity is obliged by the exemption decision to report any change of decisive facts;

How is secured and in fact fulfilled the limitation on transactions by a single customer pursuant to Section 34 para 2 letter c) of the AML Act, i.e., max. EUR 1,000 per 30 days.

3.2.2 SUPERVISION BY THE CNB

Application of the risk based approach in supervision of the AML/CFT area by the CNB

The FATF review in 2012 introduced the emphasis on the requirement to apply the risk-based approach in all AML/CFT areas at the national level, at the level of supervision and at the level of financial institutions. This principle has become part of the EU law through the Directive 2015/849 of the European Parliament and of the Council. The requirement to apply the RBA is reflected in the amendment to Act No. 253/2008 Coll., on Certain Measures against the Legalization of Proceeds of Crime and the Financing of Terrorism, as amended. The CNB implements the RBA principle in line with the CNB's Long-Term Supervision Concept as well as when planning and performing AML/CFT. The CNB performs AML/CFT supervision not only through on-the-spot checks, but also through remote surveillance, carried out by checks of fulfilment of remedial measures to remove identified weaknesses from on-the-spot checks and assessing systems of internal policies of supervised entities.

1. Application of the RBA in compiling the CNB's control plan in the area of AML/CFT

In order to effectively perform supervision the CNB has long been using the system for comprehensive risk assessment of financial institutions. Based on the risk assessment of supervised entities, the supervision focuses on the performance of its activities, allocates resources, chooses supervisory tools and communicates its requirements to supervised institutions and other supervisory authorities. This comprehensive assessment takes into account, i.a., the assessment of the level of implementation of selected AML/CFT measures in a financial institution concerned.

The RBA is thus reflected in the preparation of the AML/CFT audit plan of the CNB. Other factors for the compilation of the control plan are especially the information obtained in cooperation with the FAU and with the foreign supervisory authorities and findings from the public.

2. Application of the RBA in the CNB performance of AML/CFT supervision

The CNB applies the RBA, not only in setting up a control plan, but also in performing on-site visits. The subject of on-site visits is all key areas of adopted and implemented AML/CFT measures of supervised financial institutions. In particular, AML/CFT processes are analysed and their quality and sufficiency, compliance with legislation and effectiveness of internal control mechanisms are also assessed. The spectrum of findings from AML/CFT supervision is relatively broad. The CNB therefore makes a distinction between a systemic or individual breach and from this perspective assesses their impact on the quality of risk management of the audited entity. The audited entity is also informed of the on-site visit outcomes.

Performance of on-site visit is governed by the principle of proportionality across sectors while maintaining a uniform supervisory approach for all institutions with a similar scale and complexity of activity.

3.2.3 SUPERVISION BY THE CTIA

Czech Trade Inspection Authority (hereinafter only as “CTIA”) is a public body subordinate to the Ministry of Industry and Trade. CTIA has been established by the Act No. 64/1986 Coll., on the Czech Trade Inspection Authority. CTIA controls and supervises legal and natural persons selling or supplying products and goods on the internal market, providing services or performing similar activity on the internal market, operating a marketplace (market), unless another administrative authority exercises this supervision under special legislation.

The CTIA, i.a., to a specified extent, supervises the compliance with obligations under AML Act, namely the obliged entities under Section 2 para 1 letter j) (persons authorized to trade in items of cultural heritage or cultural value or to broker such trades) and furthermore persons under letter (k) (persons authorized to trade in used goods or to mediate such transactions or to accept pledges). Although the CTIA performs control of compliance with the AML Act all year round, two on-site visits focused specifically on bazaars, pawnshops and car-shops were included in the control plan last and this year. The on-site visits checked the compliance with obligations of the seller stemming from the generally binding legislation when offering and selling used goods. The “Autobazars” control action covered the supply and sale of used passenger cars. In these specific on-site visits, CTIA inspectors also focused on checking compliance with Section 7 para 2 letter f) of the AML Act, i.e., the seller's obligation to identify the customer. This violation of the AML Act is detectable in particular in the seller’s documentation. The outputs from the inspections show that the sector – bazaars and pawnshops – is more problematic. Findings from the inspections on money laundering showed that risk is posed, in particular, by the large number of entities operating in this sector.

As these inspections have also revealed a higher percentage of breaches of generally binding legal regulations within the scope of competence of the CTIA, in particular of Act No. 634/1992 Coll., on Consumer Protection, these specific control actions will be included in the control plan of the CTIA also in 2017. The CTIA will seek to contribute to mitigating the risks of money laundering in the sectors and will continue to thoroughly supervise the compliance of obliged entities with the AML Act.

3.2.4 NATIONAL ORGANIZED CRIME AGENCY CPIS

The documents for the NRA were prepared for the Police of the Czech Republic as a whole and according to the scope of competence of individual organizational units. The Serious Economic and Corruption Crime Command of the Criminal Police and Investigation Service (SECCC CPIS) for the purposes of the national assessment of the risk of money laundering and terrorist financing analysed serious economic crime within its competence according to Mandatory Order of Police President No. 103/2013 Coll., i.e., on the national level. The Organized Crime Unit, Criminal Police and Investigation Service (OCU CPIS) addressed for the NRA terrorism financing.

Since 1 August 2016, services with national operation have been reorganized. SECCC CPIS and OCU CPIS were merged and a unit called the National Organized Crime Agency (NOCA CPIS) has been established. As of the above date, the Mandatory Order of the Police President No. 103/2013 Coll., on fulfilment of selected tasks of the police bodies of the Czech Police in criminal proceedings, has been updated. The merger concerned two units that detect, verify and investigate offenses at national and international level. One of the units focused on economic crime and the other one on organized crime. By merging these two services, the Police Presidium has sought to streamline criminal proceedings and has reflected on the long-term trend of proliferation of organized crime to areas of economic crime as well as the fact that organized crime (criminal groups) no longer focuses only on a certain area of crime (e.g. taxes), but illegal activities are carried out in various areas of general, property and economic crime.

3.2.5 THE ROLE OF CUSTOMS ADMINISTRATION IN COUNTERING ML/TF RISKS

The Customs Administration of the Czech Republic is a security corps with competences in the field of administration of customs and certain taxes, as well as other non-fiscal activities in the benefit of the state and its citizens. It is subordinate to the Ministry of Finance.

Customs administration is a comprehensive administrator of excise duties (taxes on: alcohol, beer, wine and intermediate products, mineral oils, hydrocarbon fuels and lubricants, tobacco and tobacco products; environmental taxes) and

at the same time, the Customs Administration is a law enforcement authority with a substantive jurisdiction in proceedings on offenses committed by breach of customs legislation and regulations on the import, export or transit of goods, even in the case of crimes committed by members of armed forces or security corps; as well as violation of legislation on the placement and acquisition of goods in the EU Member States when these goods are transported across the national borders of the Czech Republic and in case of violation of tax regulations, if the Customs Authority is the tax administrator under special legal regulations.

In summary, the Customs Administration carries out activities in the areas of:

a) Administration;

b) Customs;

c) Tax administration (full scale excise duties administration, administration of VAT in the case of illegal import of goods and in import of goods by tax non-taxable persons);

d) Control and supervision;

e) Police authority.

The so-called dual status of Customs Administration as a tax administrator and a law enforcement authority can be considered as its strength. Concurrence of criminal and tax proceedings in this case can only take place under conditions stipulated by the law, i.e., both from the point of view of the legal authority of the tax administrator to provide information from tax proceedings to a police body, as well as from the point of view of the tax administrator's authorization to access a file in accordance with criminal law.

The most frequent cases with respect to the breach of customs and tax regulations which have been identified by customs authorities include:

1. Cases of illegal handling of unmarked alcohol are the most common form of violation of legal regulations in the field of alcohol tax administration. The illicit production and distribution of alcohol and spirits outside the tax warehouse register were also recorded. Violation of legal regulations has also been detected with respect to still wine. The cases related to the import of this commodity from another EU Member State into the Czech Republic and its subsequent putting into circulation unduly marked by another trademark.

2. One of the primary objectives of the Customs Administration is the fight against illegal cigarette production and, at the same time, illicit processors of tobacco leaves for tobacco for smoking and supplying illicit tobacco factories in the Czech Republic and other EU Member States. The fight against illegal trade requires close international cooperation, operational exchange of information, establishment of transnational investigation teams and cooperation with legal tobacco producers. There are three directions in the long run to detect the aforementioned illegal trade. There have been minor changes in the mode of transport; the status quo is maintained in shipping routes. Non-original and original tobacco products, which use the sales price differences in the Eastern and Western markets, are transported along the Eastern European route.

   The East European route is made up of the former Soviet Union countries, Poland and Slovakia. Original cigarettes of renowned manufacturers, as well as original cigarettes from local producers in Belarus, Ukraine and the Russian Federation, are flowing along this route to the Czech Republic. These illegal shipments use the differences in prices in the country of production and in the country of sale (countries of production are, as mentioned above, Ukraine, Russia and Belarus). The illegal cigarette production is flowing into the Czech Republic also via the Baltic States; counterfeit cigarettes originating in Asian countries (China, Vietnam) are imported. To the Baltic countries, these goods arrive via ships heading from Asia to seaports in the Baltic and through the northern branch of the Trans-Siberian Highway. Cigarettes are shipped to Poland and are divided into deliveries that continue to the EU. The detection of illegal transport of tobacco and tobacco products on this route takes place within the Czech Republic. In this respect, the Customs Administration has sufficient powers to control selected products subject to excise duty.

   Another way to detect illegal tobacco and tobacco products trade is to track the Asian route, which is made up of Asian countries (China, Vietnam) and by Western European and Southern European ports. In particular, counterfeit cigarette of renowned brands and tobacco for illegal cigarette production are smuggled from Asia. The shipping is carried out in sea containers, which are further transported in road and rail transport. There is a decrease in detected cases on this route. The probable cause is the diversion of routes from seaports in Germany and the Netherlands to southern European ports; especially to ports in Greece and Bulgaria. These countries do not have the appropriate RTG technique as Western European ports. Cooperation with these countries is significantly lower than cooperation with the customs authorities of Western European countries.

3. In the area of third-country trade, the mode of committing crime has not changed compared to previous period. The main causes of illegal activity in the area of customs and abuse of regime 4000 and 4200 for import of goods in the Czech Republic are mainly in the legal system of the Czech Republic which allows for rapid establishment of legal persons and their registration on the basis of powers of attorney. A negative aspect is also that companies are not deregistered after tax evasion and can be repeatedly used to commit fraud. Another negative factor is that companies in the Czech Republic may not own any capital.

   In the Czech Republic, there are 27 groups dealing with mediation or securing imports of goods from Asia to Europe, according to available information. The

established facts show, that the Czech Republic is only a transit point of imported goods, which is then exported to the rest of Europe and only a fraction of the imported goods remain on the territory of the Czech Republic. Illegal activity in the field of customs is, in particular on highest levels of criminal chains directed by the Asian community, which is aware of the high latency of its illegal activity and exploits the absence of territoriality. Criminal groups rely on "good relations and customer approach" of customs offices concerned when dealing with imported goods and also exploit weaknesses in the system – e.g., transferring companies declaring imported goods at customs offices with a heavy workload in order to facilitate customs clearance of goods where there is less risk of detection. Criminal groups can also be characterized as flexible and highly organized with well-defined areas of their activities, such as logistics, document production, financial transaction security, customs clearance.

Customs and tax frauds on the import of goods from third countries by way of abuse of the 4000 customs regime, e.g., to underestimate imported goods on the basis of fictitious invoices. These are deliberately created new documents on the price of goods. The document shows lower value of the imported goods than actually paid. The value is adjusted to be slightly above the threshold set by the control systems. Another typical feature of the above-mentioned frauds is the circumvention of control systems by exploiting companies authorized to use simplified system and the possibility of importing goods outside the customs office's working hours, thereby minimizing the risk of control by customs authorities. Another example of customs fraud is the reduction of contractual and anti-dumping duties in connection with declaration of incorrect origin of goods when importing fasteners into the Czech Republic and thereby benefiting from unilateral and bilateral agreements.

With respect to joint measures of the Customs Administration and the Financial Administration of the Czech Republic, such as calling into question the customs value of goods, criminal investigation, the issue of protective orders and performance of on-site execution immediately after the release of the goods leading to the fulfilment of the tax obligation, there has been decrease in ratio of goods imported under 4000 regime, which is being replaced by imports under the 4200 regime, especially from Slovakia. Currently ten to fifteen trucks are arriving in the Czech Republic under this regime. According information from the Slovak Financial Administration, 43 entities are registered in Slovakia for which the 4200 regime was applied (in the period from January to August 2015 in the amount of CZK 623 million), of which 9 entities show the risk of non-payment of the tax.

The disadvantige of the 4200 regime is the absence of interconnection of customs databases across EU Member States (as opposed to VIES), making it more difficult to coordinate the exchange of information and pose a possible risk of tax fraud on VAT not only on imports, or exports of goods, but also within intra-communitarian trade. In order to detect tax evasion, there is a need for greater cooperation between customs and financial authorities at international level and the solution would certainly be to unify customs and tax collection at customs proceedings.

The Primary task of the Customs Administration of the Czech Republic for 2016 in the field of internal security, is to prepare the General Directorate of Customs to extension of its competences in criminal proceedings in the years to come (2016-2019) and, to that end,

strengthening and organizational transformation of the national authority as of 1 July 2016. The objective is to create a single authorized customs administration that will be responsible for detecting serious crimine within its full scope of competence to investigate criminal activities in a more effective way of managing activities as a police authority. The relevant legislative amendment will be submitted to the Chamber of Deputies by the Government of the Czech Republic in the near future (January 2016).

3.2.5.1 CROSS-BORDER TRANSPORT OF CASH

In general

The Czech Republic has payed considerable attention to the issue of the transfer of funds across the EU for a long time. The subject matter is regularly monitored by state authorities in the context of current developments and new trends. Legislative, safety and technical measures are subsequently adopted in this area. The aim of these measures, which also reflect FATF Recommendation 32, is in particular to prevent money laundering and terrorist financing. In this context, regular communication and cooperation between the Customs Administration of the Czech Republic and the Financial Analytical Unit of the Ministry of Finance is essential.

When implementing 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, the Czech Republic identified two risks that were not regulated by the Regulation and autonomously introduced legislative measures to eliminate the identified risks. Specifically, these two risks are:

Obligation to comply with the reporting obligation for the transport of postal and other consignments

Generally, in the Czech Republic there is a legal obligation for natural and legal persons when entering the Czech Republic from outside the EU and when leaving the Czech Republic to such a territory to declare in writing the customs authorities of the import and export of valid Czech or foreign currency, travellers cheques or money orders convertible into cash, bearer or registered securities, as well as other investment instruments that are signed but do not include the payee's name, with a total value of EUR 10 thousand or more.

However, there are other ways of transporting funds that can escape the attention of state authorities. The Czech Republic has identified postal and freight transport as risk areas. Following the risk assessment, it was decided to extend the legal provision and implement the notification obligation for postal and other shipments. At present, a legal obligation is imposed on those dispatching from the Czech Republic outside the territory of the European Union or receiving mail or other consignment of a total value of EUR 10 thousand or more, to notify customs authorities of this consignment and to ensure that the consignment is presented for inspection.

The fact that the EU is currently preparing a change to the above-mentioned Regulation 1889/2005 proves the timely identified risk. One of the proposed changes is the extension of the above-mentioned Regulation for the obligation to declare postal and freight transport.

Obligation to declare sublimit cash

Another risk area that has been identified and which is not directly addressed by this Regulation is so-called smurfing. This is an activity where financial transactions are divided into smaller transactions in order to avoid reporting requirements for the cross-border transfer of funds. Smurfing is often associated with money laundering, terrorist financing, fraud, or other financial crimes and the relevant authorities should monitor it.

In order for the Czech Republic to monitor the transfer of funds, it was necessary to establish a legal obligation in this area. For this reason, a notification obligation has been set for persons in cases where they import or export from the EU or receive or dispatch in a consignment during 12 consecutive months items with a total value of EUR 10 thousand or more.

In practice, an electronic on-line database is in place for all cases where the customs authority has identified a passenger transferring funds in the amount of EUR 5 thousand to EUR 9,999. If this passenger is again inspected during the next 12 months and his cash amount exceeds the amount of EUR 10 thousand, the passenger violates notification obligations and is subject to administrative proceedings.

This system in the Czech Republic has decreased the number of transfers aimed at avoiding the notification obligation.

However, it is necessary to mention another identified risk that has not yet been solved and its complex solution is very difficult. In general, the notification obligation is set for a physical person without a more precise specification. This is often abused and cash is divided among family members (often very young children) and fellow travellers. The aim of dividing these amounts is again to avoid the notification obligation. One of the possible solutions is to determine the age of eligibility to fulfil the notification obligation. This particular risk will be of interest in order to eliminate it.

Intracommunity controls

The above risks have been identified and largely eliminated. However, the notification obligation applies to the transfer of funds across the EU. From the geographical position of the Czech Republic, it is clear that controls on compliance with the notification obligation are only carried out at international airports, since the Czech Republic has no external borders with third countries. Controlling and monitoring the transfer of cash across the Czech Republic is currently not regulated and there may be some risk of abuse of the set system where funds can be transported across the Czech Republic for money laundering or terrorist financing purposes.

The Czech Republic is aware of this risk. That is why in 2015 negotiations among the relevant authorities concerned were initiated in order to prepare a legislative proposal introducing control and monitoring of the transfer of cash across the Czech borders. The aim of the intended system is to obtain a legitimate tool for competent authorities to carry out this

oversight and control. In particular, it is possible to request clarification and proof of the origin of the transferred cash and possible seizure and withdrawal of cash.

The purpose of implementing the system is to strengthen competencies in the given area and to eliminate risks in connection with today's threats, which are very often financed by money from illegal activities.

Situation on the side of the FAU

The Customs Administration transmits the Notification of the transfer of funds electronically in daily updates via a dedicated secure channel of the FAU. The FAU processes and stores these batches into a database. Information on the transfer of funds is displayed in the internal information system of the Unit at each notified entity. Upon receipt of a STR under the AML Act, all reported and acting persons will be checked for presence in the cash transfer database and the result is reported to the processing analyst. The FAU's analyst also can search a particular entity in the cash transfer database.

3.2.6 THE ROLE AND IMPORTANCE OF GFD IN MITIGATING ML/TF RISKS

The General Financial Directorate is established by Act No. 456/2011 Coll., On the Financial Administration of the Czech Republic and is the supreme authority of tax offices that perform the tax administration. Taxes are the most important income of the state budget of the Czech Republic.[31] In 2015, the Financial Administration collected CZK 670 billion, of which more than half is value added tax, the collection of which in the year 2015 amounted to CZK 322 billion. Value added tax is also the most burdened by fraud and represents the greatest risk. The commission of crime is facilitated by the nature of the tax where the taxpayer's own tax liability is formed by the difference of the tax burden on executed taxable transactions and the right to deduct the tax from the received transactions. Value added tax arrears account for 70% of all tax arrears. This is the unpaid assessed tax, as of 31 December 2015. For the approximation of VAT evasion, the most often used is the VAT gap, which represents the difference between the theoretical (achievable tax revenue in a country based on the macroeconomic data) and the actual tax revenue. For better comparability among countries, the VAT gap is expressed as a percentage, i.e., as a share of the VAT gap on the theoretical tax liability arising from the economy. The latest VAT gap estimates, published by the European Commission in September 2016, indicate the VAT gap for the Czech Republic in 2014 of CZK 61.5 billion, which is 16% of the theoretical tax liability. In 2013 this figure was estimated at 19%, i.e., CZK 72 billion.[32] According to the report of the Supreme Audit Office, this figure was 26% in 20103, i.e., CZK 105 billion.[33]

The role of GFD in mitigating risk is twofold. One of the key competences of the GFD is to contribute to the preparation of tax legislation, where efforts in this area focus primarily on the creation of preventive measures such as the introduction of a system of passed tax liability on other groups of goods and services in order to minimize unjustified tax deductions. Another preventive measure is the introduction of control reports which consist of the obligation of VAT payers every month to electronically report to the financial administration taxable transactions received and executed, which allows rapid and effective control and detection of unjustified deductions where the supplier of a payer did not a file a VAT return, or did not make the taxable transaction. This obligation for the VAT payer has been introduced since 1 January 2016. A further legislative novelty is an electronic sales record which aims at reducing the evasion of tax on output from realized taxable payments to non-payers (consumers). After its implementation, it will significantly reduce the risk of revenue cuts and thus not only decrease VAT evasion but in particular evasion of income tax.

Countering abuse of the tax administration system is facilitated by organizational methodological procedures for the delegation of administration of tax entities locally responsible to the Financial Office for the Capital City of Prague to other financial offices, less burdened by the administration of a large number of legal persons. Additionally, an

[31] For the sake of completeness, it should be noted that the Financial Administration does not collect all taxes of the Czech tax system and not all tax collection is the income of the state budget of the Czech Republic. The Financial Administration collects 38% of the state budget revenue in 2014. Furthermore, tax revenue is an essential part of revenues of regions and municipalities, which receive 33% of taxes collected by the Financial Administration.
[32] Source: Study and Reports on the VAT Gap in the EU-28 Member States: 2016 Final Report TAXUD/2015/CC/131, CASE – Center for Social and Economic Research (Project leader).
[33] Source: Supreme Audit Office (control action 14/17).

amendment to Act No. 456/2011 Coll., On the Financial Administration of the Czech Republic, selected competences of tax offices for the whole territory of the Czech Republic for the purpose of search activity in tax administration, the procedure for the elimination of doubt, tax control or other control procedures in the administration of taxes. In this case, all financial offices will be competent to perform the chosen competency. This legislation will considerably simplify the control activities in case of frauds by large supplier-consumer chain of companies spread throughout the Czech Republic. It is also worth mentioning the effort to introduce pre-registration controls, i.e., screening of new VAT payers before they are allowed into the VAT system by assigning a valid registration.

Another important task of the GFD is the analytical and coordination activity. In this area, the Risk Management Section of Tax Administration is primarily responsible for using all available public and non-public information resources for timely detection of tax fraud. In this area, the GFD is undergoing intensive development which, i.a., enables the effective linking of data from control reports to detect carousel fraud. To illustrate how important effective analytical activity is, consider that there are over 500,000 active taxpayers registered in the Czech Republic and the Financial Administration employs more than 3,000 control officers.

Coordination activity is equally important, as large chain fraud always operates across regions. Perpetrators move their activities easily from one part of the Czech Republic to another, which is facilitated by office houses that provide fictitious seats to legal persons. The Risk Management Section of Tax Administration is responsible for the coordination of the fight against tax evasion among the Financial Administration, the Customs Administration of the Czech Republic and law enforcement authorities. Their joint project called Tax Cobra was successfully launched in 2014. The Tax Cobra project was extended from the central level to the regional level in 2015. Cooperation with the Financial Analytical Unit of the Ministry of Finance is also successful, which confirms the importance of early information on suspicious bank transactions in the fight against carousel fraud, in particular in securing payments for unpaid tax for companies in the position of missing trader. In 2015, thanks to this cooperation, CZK 1,411 million (in the sense of the unpaid tax, which was calculated based on the findings from the FAU at CZK 3,613 million) was drawn from proceeds of tax evasion.

3.3 IDENTIFICATION AND ASSESSMENT OF VULNERABILITIES ARISING FROM PESTEL ANALYSIS ACCORDING TO FATF METHODOLOGY

3.3.1 CORRUPTION AS A VULNERABILITY RELEVANT FOR ML/TF RISKS

The study of the National Economic Council of the Government (NERV) shows that only corruption in relation to the state budget causes damage in the order of tens of billions of crowns (estimate for 2010 - CZK 39 billion).[34] Revenues from this type of crime are of considerable value. Thus, perpetrators of corruption naturally face the question of how to launder proceeds of crime. The high level of corruption represents a significant vulnerability in ML/FT risks. Reasons can be seen in particular in the following facts:

- Corruption is not only an predicate offence for money laundering, regardless of whether such proceeds are generated and laundered in the Czech Republic, or whether they were generated in other countries and are subsequently placed in the Czech Republic, invested with the aim of legalizing;[35]
- Corruption is also an important tool for committing other crimes and for legalization as such;[36]
- Last but not least, it cannot be neglected that the financial system, or designated non-financial businesses and professions under the AML Act may be abused to provide funds for subsequent corruption or directly to pay a bribe.[37]

Corruption is a serious crime, i.a., for the following reasons:

- It is often part of organized crime;
- It generates significant proceeds;
- It causes considerable indirect damage, such as increasing public budgets, damaging confidence in the functioning of the rule of law, hampering the development of infrastructure, increasing prices of services provided (all of which can be mutually supportive).

The Czech Republic is aware of this risk and pays considerable attention to corruption issues in its strategic documents.[38] The measures currently being discussed and adopted, which

[34] Source: NERV Study Kohout, P. (ed.) et coll.: Countering Corruption. Colection of texts by working group on countering corruption of the National Economic Council of the Government (Národní ekonomická rada vlády (NERV)). Prague: Office of the Government of the Czech Republic, National Economic Council of the Governemtn (NERV), 2011.
[35] See examples in the Chapter on Identification of Threats.
[36] See examples in the Chapter on Identification of Threats, where involvment of insiders from the public or private sphere (possible gatekeepers, internal fraud) is possible.
[37] See examples in Chapter on Identification of Threats or sings of susspicion and risk factors in guidance sections of chapters on vulnerabilites in the private sector. FAU draws attention to this aspect in its educational activity.
[38] In this context, in particular the Government Concept of Combating Corruption, the Action Plan to Combat Corruption and basic principles of combating corruption should be recalled. http://www.korupce.cz/cz/protikorupcni-strategie-vlady/na-leta-2015-2017/strategie-vlady-v-boji-s-korupci-na-obdobi-let-2015-a-2017-119894/

should substantially reduce corruption in the Czech Republic, include in particular the following:

- **Financing of political parties and election campaigns** (amendment of Act No. 424/1991 Coll., on association in political parties and political movements and amendments to electoral laws)

The aim of this Act, promulgated in the Collection of Laws under No. 302/2016 Coll., is to strengthen the transparent functioning of political parties and political movements. The proposal provides, i.a., for the establishment of the Office for the Supervision of the Financing of Political Parties, whose primary task will be to monitor compliance with statutory obligations of political parties and political movements.

- **Proposal of Act on Proof of Origin of Assets**

Pursuant to Act No. 321/2016 Coll. is to modify existing tax law mechanisms so that it is possible to detect unreturned or concealed incomes of taxpayers and then tax them.

- **Amendment to the Criminal Code implementing the so-called confiscation directive**

Following the Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the confiscation of instrumentalities and the proceeds from crime in the European Union, specifically its requirement to introduce so-called enhanced confiscation powers, it is proposed to introduce a new safeguard measure of seizure of a part of assets, which would allow for the total or partial confiscation of assets of an person convicted of an intentional crime that may have directly or indirectly lead to economic benefits, if the court, based on the circumstances of the case, including specific facts and available evidence, such as that the value of the assets is disproportionate to the legal income of the convicted person, considers that the assets come from criminal activity. The safeguard measure of seizure of a part of assets is intended to affect assets that have strong indications of its "criminal" origin so as to prevent further crime and to seize assets likely to be derived from unspecified crime. The proposal implementing this directive is currently being discussed by the Chamber of Deputies as a Parliamentary Press No. 753.

- **Proposal of Act on Public Prosecutor's Office**

The proposal on the Public Prosecutor's Office (Parliamentary Press No. 789) regulates fundamental issues of activities and organization of the Public Prosecutor's Office, its status, roles and responsibilities of individual prosecutors. The main objectives of the new legal regulation are the effort to minimize the risk of undesirable influence on the public prosecutor's office, especially by the executive and prosecutors, as well as efforts to ensure specialization in the most serious forms of crime. The fulfilment of the later objective is to be achieved through the establishment of a completely new Public prosecutor's Office (Special Public Prosecutor's Office) with a national competence.

The proposal of Act on the Public Prosecutor's Office reflects the fact the most serious forms of bribery and crime committed in connection with public procurement or insolvency proceedings are the concomitant phenomenon of property and economic crime. Therefore,

this fact had to be reflected both in the material competence of the Special Public Prosecutor's Office and in the personnel structure of this specialized public prosecutor's office, which will require a more comprehensive specialization of public prosecutors in the field of economic crime, as well as deeper working experience of individual public prosecutors and a multidisciplinary approach. Thus, this Public Prosecutor's Office will be primarily responsible for supervising the lawfulness of the pre-trial procedure and the first and second instance proceedings in matters of crime against property and in matters of economic harm or property benefit of at least CZK 250 million or for such crimes committed for the benefit of an organized criminal group and for offenses related to the promise, offering, granting, receiving or requesting bribery and offenses committed in connection with public procurement or insolvency proceedings.

The jurisdiction of the Special Public Prosecutor's Office will also be given in respect of offenses related to the participation on a crime and legalization of proceeds of crime (committed in both deliberate and negligent form) if the predicative offense is one of the above-mentioned crimes. In addition to this mandatory jurisdiction, modification of the so-called optional faculty of the Special Public Prosecutor's Office is proposed. The SPPO may decide that it is competent to supervise the observance of lawfulness in the pre-trial procedure and to public defence in court proceedings in criminal matters against property and in economic matters, even if the damage or property benefit does not reach the limit of CZK 250 million or it is not property or economic crime committed for the benefit of an organized criminal group and in criminal offenses under Chapter IX of the Criminal Code and the related crimes of participation and legalization of proceeds of crime (both committed in a deliberate and negligent form).

- **Act on the Register of Contracts**

On 1 July 2016, the Act on the Register of Contracts (340/2015 Coll.) entered into force, the primary purpose of which is to defend against overpriced public contracts, unnecessary purchases or disadvantageous sales of property. In addition, the law should provide sufficient ovesight over the economic management of state property not only by the responsible administrative authorities but also by the general public.

- **Amendment to the Act on Conflict of Interests**

The Parliament of the Czech Republic also approved a government proposal amending Act No. 159/2006 Coll., On Conflicts of Interest, as amended (Parliamentary Press No. 564). This proposal includes the introduction of an obligation to declare activities, assets, income and liabilities as of the day before the date of office, streamlining the control mechanism, tightening sanctions, computerizing the whole agenda and extending the range of former public officials restricted in the transition from the public to the private sphere.

- **Act on Public Procurement**

Act No. 134/2016 Coll., On Public Procurement, which came into effect on 1 October 2016, stipulates a general obligation for the contracting authority to act in such a way that there is no conflict of interest during the entire procurement procedure, while the number of persons to whom this obligation apply is defined by their ability to participate in the procurement

process (on the part of the contracting entity) or their possibility to influence the outcome of the procurement procedure.

The contracting authority must ensure that all its decisions and other acts which may affect the award of the contract or the exclusion of tenderers are made only in the light of the objective needs of the contracting authority and have not been influenced by the financial or other personal interest of persons participating in the procurement process or person that may affect its outcome.

The Act further regulates the property structure of suppliers. It will be the responsibility of the contracting authority to investigate whether the selected contractor (joint stock company) has other than book-entry shares. In the case of anonymous owners with a Czech contractor, the contracting authority will be required to exclude such a winner from the procurement procedure in accordance with Section 48 para 7 and para 9 of the proposal. For foreign contractors, the contracting authority must identify owners of shares above 10%.

In accordance with Section 104 para 2 of the Public Procurement Act, the contracting authority is also obliged to require from the selected contractor as a condition for the conclusion of the contract the submission of documents on its ownership structure up to beneficial owners according to the AML Act.

- **Amendment to the AML Act**, which, i.a., transposes the 4th AML Directive

The amendment to the AML Act further specifies the measures described below, which play an important role in the fight against corruption:

- The extension of the definition of politically exposed persons for domestic PEPs; only foreign PEPs have been covered by the current Act and the obliged entities are, i.a., required to identify PEPs and apply increased prudence to these persons as part of CDD;
- The coverage of virtual currency service providers, which is motivated, i.a., by the possible vulnerability (not yet detected threat) to abuse to provide funds for bribery;
- Reduction in the amount of cash payment at which all entrepreneurs must identify their customer (from EUR 15 thousand to 10 thousand);
- Specification of the beneficial owner definition; and
- Obligation of legal persons to know their beneficial owner.

Amendment to the AML Act will be effective from 1 January 2017.

- **Amendment to the Act on Public Registers**, which is legislatively related to the above-mentioned amendment to the AML Act.

The aim of this amendment is to establish a non-public record of data on beneficial owners of legal persons and trusts, which will not be a public register. Register should serve primarily as a tool for possible use in the execution of CDD under the AML Act. Competent public authorities and obliged entities under the AML Act will have a remote access to the information on beneficial owners. The range of subjects with access to the data on beneficial owners will therefore be very wide. Additionally, any entity may obtain an extract from the

register if it proves an interest in preventing selected offenses (including ML and TF, predicate offence and participation, including by negligence). The register of beneficial owners, will allow legal persons registered in public registers will be allowed to uncover their ownership structure. The Register will allow legal persons to obtain an extract for further use.

The amendment will be effective as of 1 January 2018.

- Last but not least **The CZ10 Project: Project to strengthen the fight against corruption and money laundering in the Czech Republic (Norway Grants: 2009 – 2014)**

Besides other activities, the FAU is also the final beneficiary of the CZ10 Project under the Norway Grants (www.cz10.cz). The project is divided into four areas, where partial activities - workshops, conferences, studies, analyses and foreign study visits are organized. The implementation of the project started in September 2014 and the end of its implementation is scheduled for July 2016. By March 2016, 599 representatives from the MF, MoJ, MoI, the Czech Police, courts, the Public Prosecutor's Office, NPOs and other representatives of, in particular the public sector.

The first thematic issue was identification and comprehensive understanding of risks and threats related to corruption and related crime in the Czech Republic. The conflict of interests and the issue of beneficial owners of legal persons and trusts were identified as potentially the most risky. A study was prepared on either of the two topics, both of which are publicly available on the project's website. The recommendations and conclusions were presented at a separate workshop.

The second thematic issue was the issue of proposals to improve criminal law in the fight against corruption and the fight against money laundering. A training manual on the criminal liability of legal persons, a comparative study on Czech, German and UK legislation in the area of seizure of assets were, i.a., made.

The third thematic issue was to ensure the transparency of the funding of election campaigns and of the candidacy of independent candidates. This issue is also contained in the amendment to the Act on Financing of Political Parties and Election Campaigns. The project was used to make a comparative study of the proposed Czech legislation with legislation of Estonia, Poland, Great Britain, France and Ireland. The last thematic issue is the protection of the whistle-blower, in which an analysis was developed evaluating the need for a whistle-blower centre in the Czech Republic.

3.3.2 VULNERABILITY OF NON-PROFIT ORGANIZATIONS IN TERMS OF ML/TF

Non-governmental non-profit organizations (NPOs) are legal persons of private law, of both corporate and foundation types (comp., legal persons of public law such as municipality, region, state, professional organizations). As is clear from its designation, NPOs are legal persons independent of the State or other public-law corporation and their primary purpose, unlike commercial corporations, is not to distribute profits among their members, but rather a general (public) profitability or the development and protection of private interests.

NPO is not a legal concept but an overarching concept for legal persons of diverse legal forms. Generally speaking, NPOs include legal persons of these legal forms[39]:

- Association (formerly a civic association), or a subsidiary association;
- Public Benefit Company;
- Institute;
- Religious legal persons[40];
- Foundation;
- Endowment;

Similarly, as business corporations (such as a limited liability company) are abused to commit predicate offence and subsequently to conceal the illegal origin of criminal proceeds, NPOs may also be exploited and abused.

Vulnerabilities

With respect to predicate offence, fraud with public or European subventions often takes place. In the subsequent legalization of proceeds of crime, or in the financing of terrorism, the fact that NPOs are generally not subject to such broad demands for the transparency of their activities, as is the case with business corporations, is exploited. This is also evidenced by foreign experience of abusing NPOs for the purpose of supporting and financing terrorism.

The lack of regulation of the non-profit sector from the point of view of ML/TF risks has been repeatedly criticized by the Moneyval Committee of Experts, most recently in the fourth evaluation visit in April 2011. The Moneyval Committee has evaluated the non-profit sector as

[39] State policy towards NPOs for the years 2015-2020, approved by Government Resolution No. 608 of 29 July 2015. http://www.vlada.cz/cz/ppov/rnno/dokumenty/statni-politika-vuci-nno-na-leta-2015---2020-133505/

[40] For the purpose of this Report, the term is used to a wider extent, comprising:
Churches and religious societies;
Unions of churches and religious societies; and
Registered legal persons;
Authorities of registered churches and religious societies, religious and other church institutions of persons claiming allegiance to a church and a religious society, established for the purpose of confessing religious beliefs;
Purpose-built facilities of registered churches and religious societies, established for the provision of social or medical services or acting as charities or deacons.

only partially compliant with the FATF Recommendations. The absence of comprehensive knowledge of domestic NPOs, lack of oversight and lack of transparency of their funding has been criticized in particular. The absence of a publicly available list of civic associations has long been criticized not only on the part of European experts.[41]

Adopted Measures

Within the framework of the process of recodification of private law, Act No. 304/2013 Coll., on Public Registers of Legal and Natural Persons (hereinafter referred to as the "Public Registers Act" or "PRA") has been effective since 1 January 2014. The PRA substantially extended the amount of publicly available information on NPOs. This information is available online free of charge. The PRA regulates:

- **Register of Associations**;
- **Register of Foundations (foundations and endowments)**;
- **Register of Institutes**;
- Register of Housing Units Owners;
- Commercial Register;
- **Register of Public Beneficial Companies**.

The law has in principle set up a unified system of keeping public registers (with the exception of, for example, registers of church legal persons maintained by the Ministry of Culture – see below for details). Registry courts play a pivotal function in this system.

According to Section 25 of the PRA, the following are, i.a., recorded in a public register: name, seat or address of registered person, subject of activity, legal form of a legal person, date of birth and termination of legal person, identification number of a person assigned by a registry court, name of statutory body, other facts stipulated by law or important facts, the registration of which is requested by the registered person, if it has a legal interest in such registration.

An essential provision strengthening the transparency of NPOs is Section 66 of the PRA adjusting the contents of the collection of documents. According to the relevant provision, the collection of documents includes e.g.

- **Memorandum of association** of a legal person, **statute** of a foundation, **statute** of an endowment or institute, **statutes** of an association;
- **Decision on election or appointment**, appeal or proof of another termination of a function of persons who are members of a statutory body;
- **Annual report, regular, extraordinary and consolidated financial statements**, if they are not included in the annual report, if the obligation to deposit them into the

[41] Final research report Transparency of the operation of the non-profit sector in the Czech Republic with special emphasis on the prevention of its misuse for the purposes of terrorism financing. Research programme "Security Research" of the MoInt VD20062008B12.

collection of documents is stipulated by the Act on Accounting (Note: Section 21a of Act No. 563/1991 Coll., on accounting) and if they're production is required by a different law (Note: Act No. 89/2012 Coll., the Civil Code, hereinafter referred to as "CC").

Penalties for non-compliance in relation to a public register

Pursuant to Section 104 of the PRA, the President of the Chamber is entitled to impose a fine of up to CZK 100 thousand in the event of failure to disclose the facts or the filing of a document necessary for a decision in a procedure initiated without a proposal or a call to submit documents to be deposited in the collection of documents. In case of repeated failure to fulfil this obligation, if there is a legal interest therein and if it can have serious consequences for third parties, the Registry Court may, under Section 105 of the PRA, initiate proceedings on the cancellation of the registered person with liquidation.

The described legislation is very positive with respect to the transparency of functioning of NPOs. However, on the basis of experience of fulfilling obligations in relation to the Commercial Register,[42] it is possible to doubt the fact that the collection of documents will be properly fulfilled by the registered persons. The law provides the courts with number of possibilities to deal with failures in fulfilling these obligations (see above). However, in view of the large number of persons who have been newly registered in the Registers, it is not principally possible to check in advance whether the electronically transmitted documents are actually those documents to be stored in the public register. At the same time, legal regulation and the technical functioning of public registers are not set up so as to quickly and timely reveal a mere formal fulfilment of obligations by sending blank electronic documents.

Implementation of the newly revised FATF Recommendation R.8

In June 2016, the FATF issued revised Recommendation R.8 and related Explanatory Note. It highlights the importance of community service and the number of services provided by NPOs in a number of countries around the world. It also describes the risk of abuse of a vulnerable NPO segment to support and finance terrorism and recommends that governments introduce a range of risk mitigation measures within the risk-oriented approach.

Despite the fact that the risk of abuse of NPOs to support and fund terrorism is currently a risk rather considered and not yet detected, the threat is so serious that we need to address vulnerabilities that could be exploited by the threat. In order to find a reasonable balance between the development of the non-profit sector and the protection of human rights, on the one hand and mitigating the risks of support and financing of terrorism, on the other hand,

[42] Report on the Ombudsman's inquiries – research on the fulfillment of the collection of documents http://www.ochrance.cz/stiznosti-na-urady/pripady-a-stanoviska-ochrance/stanoviska-statni-sprava-soudu/ostatni/
The analysis of the Ministry of Justice was elaborated in cooperation with the Ministry of Interior and the Police of the Czech Republic "Possibilities of Provision of Information on Structures of Legal Persons and Other Entities to Law Enforcement Authorities" approved by Government Resolution No. 775 of 16 October 2013.

the authorities concerned have agreed to implement this Recommendation. As part of the initial discussions, a number of mitigating measures have been identified, of which a large part is already being implemented. In addition, there are a number of measures already planned, as well as some measures, the specific wording of which must be based on more detailed discussions taking into account in particular the feasibility and proportionality of such measures to the seriousness of the risk. Last but not least, account should be taken of the fact that the risks are dynamic and that the risk of abuse of NPOs to TF may also change.

Measures already in place:

1/ Promoting transparency and mitigating risks on entry into the non-profit sector:

All legal persons registered in a public register (within the meaning of the PRA) are obliged to communicate to the Registry Court facts and submit documents necessary for a decision in a procedure initiated without a proposal and submit documents to be deposited according to the law to the collection of documents. Certain general infrastructure for identifying and requesting information on NPOs already exists.

The Registry Court may impose a legal fine on a legal person up to CZK 100 thousand if it did not comply with those obligations even after the Registry Court had requested it (Section 104 of the PRA). If a legal person fails to comply with these obligations repeatedly, or if such a breach may have serious consequences for third parties and there is legal interest, the Registry Court may, of its own motion, initiate proceedings on the cancellation of a registered person with liquidation. The non-observance of the call with serious consequences for third parties is in particular the failure to submit updated documents under Section 66 letters a) to c) and j) of the PRA. This is for example the founding law, the decision on the election of a member of the statutory body, the financial statement, the annual report, etc. (Section 106 para 1 of the PRA).

The Registry Court may also cancel a legal person and order its liquidation upon proposal submitted by a person, who proved a legal interest therein, also without a proposal, but after fulfilment of certain conditions. The cancellation of a legal person by the Court is possible, if the legal person pursues illegal activity to such extent, that it seriously undermines public order (in particular unauthorized activity pursuant to Section 145 of the CC). Furthermore, a legal person may be abolished if it no longer fulfils statutory conditions required for the establishment of a legal person or in the absence of a quorum of a statutory body longer than two years. A legal person may also be cancelled if explicitly required by law. As for abolition of a legal person by the Court for a reason that can be mended, the Court first sets an adequate period for the legal person to remove shortcomings (Section 172 of the CC). It should be recalled that the right to associate is provided for by the Charter of Fundamental Rights and Freedoms (LZPS). Section 20 para 3 of the LZPS allows for limitation of the right to associate, but only in cases defined by law, if it is necessary in a democratic society in case of state security, protection of public safety and order, prevention of offences or to protect rights and freedoms of others. With respect to registration (and establishment of defined legal persons), other limitations cannot be set.

In case of possible illegal activity of a legal person, the general codification is in the Civil Code. Section 145 para 1 of the CC stipulates that it is forbidden to establish „a legal person for the purpose of breaking law or attaining an objective illegally, in particular, if the objective is to:

a) Deny or restrict personal, political or other rights of persons based on their nationality, gender, race, origin, political or other thinking, religion or social status;

b) Annoying hatred and intolerance;

c) Support violence or;

d) Manage a law enforcement authority or exercise public administration without statutory rights.“

Pursuant to the above-mentioned, the Civil Code in its Section 129 para 1 letter c) stipulates that "a court shall declare a legal person after its creation as null and void, if the act of the founders is contrary to Section 145." Before such a decision, however, the court shall provide the legal person with a reasonable time for redress if a defect can be removed (Section 130 CC). Furthermore, according to the provisions of Section 172 para 1 letter a) CC "a court on the application of a person who has established a legal interest therein, or of its own motion, shall revoke a legal person and order its liquidation if it engages in unlawful activities to the extent that it seriously undermines public order." With respect to associations, the CC in Section 268 para 1 letter a) stipulates that "the court shall abolish the association with liquidation at the request of the person having a legitimate interest in it, or of its own motion, if the association, when notified by the court, proceeds with the activity prohibited under Section 145 of the Civil Code."

The general regulation of the Civil Code is also reflected in the procedural regulation on certain public registers (including the Register of Associations); reference can be made in particular to Section 86 letter f) of the PRA which provides that "the Registry Court shall refuse the application to register if the purpose of the constituted legal person is contrary to the provisions of Section 145 of the Civil Code".

Also church legal persons are registered in publicly accessible registers. Churches and religious societies must apply for registration if they wish to have a legal personality. Registration is carried out by the Ministry of Culture on the basis of the Act on Churches and Religious Societies and the Administrative Code. During the registration process, a number of conditions are being examined to avoid registration of groups of potentially dangerous or pursuing illegal activities. The Ministry of Culture cooperates with other authorities (such as the Ministry of the Interior, the Security Information Service) and court experts in these proceedings. Registered churches and religious societies and their information are recorded in the Registry of Registered Churches and Religious Societies, which is publicly accessible.

Unions of churches and religious societies are also subject to registration; they are registered in the Register of Unions of Churches and Religious Societies, which is also publicly accessible.

Registered legal persons, i.e., bodies of registered churches and religious societies, monastic and other religious institutions and specialized institutions of registered churches and religious societies, are registered in the Registry of Legal Persons, which is also held by

the Ministry of Culture and is publicly accessible. Access to all publicly available registries via website of the Ministry of Culture is free of charge.

If the Ministry of Culture finds that a registered church and a religious society or association of churches and religious societies is operating in violation of some of the provisions of Act No. 3/2002 Coll., on Churches and Religious Societies, which regulate conditions for activities of churches and religious societies in the Czech Republic (Section 3 letter a), Sections 5 or 27 para 5 of the Act on Churches) commences the procedure for the cancellation of registration (unless the prior notice of abandonment of this activity has been respected), as well as in cases where a statutory body of a registered church or religious society, or a statutory body of the Union of Churches and Religious Societies is not established for more than two years.

In the case of registered legal persons, the Ministry of Culture will cancel their registry if they violate relevant provisions of the Act on Churches and Religious Societies (Section 3 letter a), Sections 5 or 15a para 4) and the competent authority of the Church and the religious society, even after the Ministry's request has not remedied shortcomings, or there is no statutory body of a registered legal person for more than one year.

2/ Supporting the availability of information on existing legal persons:

The definition of the purpose of a legal person is one of the facts recorded in the public register (Section 25 para 1 letter b) of the APR). Statutory and supervisory bodies of a legal person, including its members, are also entered in a public register (Section 25 para 1 letters e), g) and h) of the PRA). The public register is accessible to everyone and everyone can view it online on the website (https://or.justice.cz/).

It should be added that, in view of the amendment to the AML Act and other related laws (e.g., the Public Register Act), the institute of beneficial owner register will be introduced into Czech law. This requirement follows from the 4th AML Directive (specifically Articles 30 and 31). According to the proposal, the Register should operate on 1 January 2018. It is proposed to create a non-public record of data on beneficial owners (as defined in Section 4 para 4 of the AML Act) to be kept by Registry Courts. Access to the register will be made available only to the legally defined range of entities, taking into account the grounds of Register, i.e., combating money laundering and terrorist financing.

All registered legal persons (i.e., for example, associations) will be required to provide information on their beneficial owners. The following should be recorded for each beneficial owner: name and address or place of residence, if different from the address, date of birth and birth number, if assigned, nationality and indication of the proportion of the voting rights, if the position of the beneficial owner is based on direct participation in a legal person, a share in the distributed funds, where the status of the beneficial owner is based on the fact that it is the recipient of funds, or other fact, if the position of the beneficial owner is otherwise established.

Churches and religious societies, as well as their special purpose facilities, are governed by general laws on accounting. According to Act No. 3/2002 Coll., on Churches and Religious

Societies, registered churches and religious societies publish an annual report on the exercise of so-called special rights and may also publish a general annual report on their activities. Special purpose facilities are required to publish annually an annual report, the content of which is defined by the Act on Churches and Religious Societies. The manner of its publication must be stated in the charter of the special purpose facility.

3/ Promotion of transparency:

The Government Council for Non-Governmental Non-Profit Organizations (RVNNO) always seeks to promote maximum transparency and openness of NPOs to the public. RVNNO creates and adjusts as necessary the so-called "Government Principles for Granting Subsidies from the State Budget of the Czech Republic to NPOs by central state administration bodies"[43]. According to this document, NPOs as recipients of subsidies are required to keep double-entry accounts (more precisely, in full or simplified scope). This document is continuously updated to reflect the current state of risk and the necessary measures. RVVNO is also engaged in awareness-raising activities to promote transparency. As part of the AML/CFT prevention, it organized seminars in the past in cooperation with the FAU and will continue to do so. Similarly, the Ministry of Foreign Affairs is systematically devoted to awareness-raising activities and will also project this specific risk in its communication with the network of NPOs involved in foreign development cooperation and humanitarian aid provided abroad. Other stakeholders, including the FAU, are also ready to engage in this awareness-raising activity.

4/ Provable record-keeping:

All above-mentioned types of NPOs as well as all legal persons with their registered office in the Czech Republic, irrespective of their purpose and activity, are an accounting unit [Section 1a of Act No. 563/1991 Coll., on Accounting - hereinafter also referred to as "AA") and each accounting unit is obliged to keep accounts. Public benefit organizations, institutions, foundations and endowment funds must compile and publish financial statements. This obligation also applies to associations (and branch associations) and church legal persons whose income or property exceeds the statutory amount. The financial statements are published by depositing them in the Collection of Documents no later than twelve months after the balance sheet date of the published financial statements (Section 21a para 2 and 4 of the Act on Accounting and Section 66 letter c) of the PRA). The collection of documents is available online on the website (https://or.justice.cz/).

Registered churches and religious societies as well as their special purpose facilities under the Act on Churches and Religious Societies publish an annual report on the performance of so-called special rights and may also publish a general annual report on their activities. Special purpose facilities are required to publish annually an annual report, the content of

[43] Approved by Government Resolution No. 92 of 1 February 2010, as amended by Government Resolution No. 479 of 19 June 2013 and Government Resolution No. 657 of 6 August 2014.

which is determined by the Act on Churches and Religious Societies. The manner of its publication must be stated in the charter of the special purpose facility.

Requirements for accounting reporting are set out in the Act on Accounting. Accounting units are required to keep accounts in such a way that the financial statements compiled on their basis are comprehensible and provide a true and fair view of the unit's accounting and financial position in such a way that a person using the information (the user), may make economic decisions pursuant to Section 7 para 1 of the AA. Accounting units prepare financial statements that are an inseparable whole and consist of the balance sheet, profit and loss statement and attachments under Section 18 para 1 of the AA. For accounting units whose main business is not an enterprise, Decree No. 504/2002 Coll., which regulates the organization, labelling and content definition of costs, revenues and financial results in the financial statements, is an implementing legal regulation to the Act on Accounting.

The Act on Accounting also sets requirements on provability of accounting records in Section 33a, including the determination of the substantive requirements of provable accounting documents in Section 11 and, last but not least, requirements for the keeping of accounting records in Sections 31 and 32 of the AA. Accounting documents shall be kept for five years beginning at the end of the accounting period to which they relate. It is important that when an entity uses accounting records for other purposes, especially for the purposes of criminal proceedings, measures against the legalization of proceeds from crime (and TF) and the like, proceed after the expiry of the custody periods specified in Section 31 para 2 of the AA, in order to ensure requirements arising from their application for the above purposes.

Transactions records are primarily secured by the Accounting Act, which sets archiving deadlines for accounting documents, which are also a tax document. In the framework of the tax audit, the tax administrator can request these documents. As regards the disclosure of records of charitable and financial activities of NPOs, they are already obliged to publish financial statements where the information is contained. In the area of donations of NPs and LPs from the point of view of tax legislation, Act No. 586/1992 Coll., on Income Taxes sets out conditions under which gifts can be provided; how they are to be proved, or rights and obligations of the donor and the beneficiary, respectively, are not set. It sets only conditions under which a gift can be deducted from the tax base (especially for what purposes and to whom the gift may be provided). The General Financial Directorate, in a legally non-binding document "Guideline GFR D-22", which provides for a uniform procedure for the application of certain provisions of the Income Tax Act, adds to this deduction from the tax base (Section 20 para 8 of the Income Tax Act) that, "Provided voluntary benefits (such as gifts) are proved by the donor by a document from which it must be clear who is the beneficiary of the voluntary benefit, the value of the voluntary benefit, the subject of the voluntary benefit, the purpose for which the voluntary benefit was provided and the date of the provision of the voluntary benefit."

In addition, a number of NPOs, in particular large foundations, on a voluntary basis, have their internal regulations regulating their work with donors and beneficiaries. RVNNO is ready to work with NPOs to develop and improve good practices to manage risks and promote accountability. This is due, among other things, to the fact that the State Policy towards NPOs 2015-2020, approved by Government Resolution No. 608 of 29 July 2015, recognizes in one of its principles donation as a manifestation of citizens' participation in public affairs

and imposes a number of tasks on RVNNO in this area. RVNNO is prepared, in cooperation with interested NPOs, to create a model code of donation that would include, among other things, the basic principles of working with donors and beneficiaries.

5/ Audit of provable record-keeping

Under Section 10 para 2 letter b) of Act No. 456/2011 Coll., on the financial administration of the Czech Republic, tax offices are administrative bodies competent to carry out supervision of compliance with obligations stipulated by accounting regulations. Tax offices also impose sanctions on accounting units for violating these regulations. Controls are carried out both on a random basis and on the basis of information obtained on possible breach of duty.

Due to the number of accounting units, area controls cannot be performed. Tax offices are addressing relevant input from other stakeholders, which suggests a serious breach of NPO's obligations under accounting legislation based on the risk based approach.

Besides, in the case of a public collection pursuant to Act No. 117/2001 Coll. on public collections, the administrative authorities check, at the end of the public collection, whether funds have been used in accordance with the declared purpose. If a public collection is held for more than one year then an annual interim statement is submitted for inspection. The Public Collection Act allows the collection to be terminated in the event of a violation of the law and the money to be transferred to the region's budget (to be used for a similar purpose).

6/ Sharing of information as a prerequisite for effective prosecution

A public register contains all essential information about each legal person (cf. Section 25 of the PRA in particular) and documents relating to, i.a., the management of a legal person (Section 66 et seq., PRA), are mandatory in the collection of documents. Similar situation exists with Registers of church legal persons and the Ministry of Culture fully cooperates with competent authorities and provide all information requested and available to it.

Investigational capacities of the Czech Police are concentrated within the National Organized Crime Agency (hereinafter referred to as "NOCA"). Within the NOCA, the Counter Terrorism and Extremism Command operates, with a specialized central communications, information and analytical department of the Police. These departments are engaged in collecting, evaluating, analysing and processing information found by the Czech Police on terrorists and persons reasonably suspected of being connected to terrorist organizations (such information may include information about suspected abuse of NPOs to support or fund terrorism). The Command is linked to all departments of the Czech Police and cooperates with other authorities concerned, including the FAU and including foreign competent authorities.

Planned measures and measures, the formulation of which will be the subject of subsequent work:

A key prerequisite for mitigating risk, applying a risk-based approach and making deliberate decisions on the application of any additional mitigation measures is the identification of risk factors and that segment of the non-profit sector that is most vulnerable to TF. For this purpose, an inter-ministerial expert group will work under the direction of the Ministry of Interior. The work of this inter-ministerial working group will also include experts from the FAU, the GFD, the Ministries of Finance, Culture, Justice, Foreign Affairs, NOCA and RVNNO.

The primary task of identifying factors and segments of vulnerability will be followed by a discussion on possible additional measures under FATF R.8 point C.6 (b). Possible vulnerabilities will be examined, for example, when receiving and providing financial support, or, for example, in some specific ways of setting up NPOs. In addition, other issues, such as the possible definition of non-governmental non-profit organizations, the concept of public benefit activity, further awareness-raising amongst the staff of the authorities involved, will be considered. The benefit of a working group thus established will also be an additional possibility of sharing information among stakeholders. Formulation of possible additional measures will always be subject to the proportionality criterion with regard to the threat of abuse of NPOs to support and finance terrorism on the one hand and the development of the non-profit sector and the constitutionally guaranteed principles of religious freedom on the other. The risk of abuse by NPOs to TF will also be consistently reflected in all key strategies such as the Government Grant Guidelines and the ZRS Strategy for the period 2018-2030.

3.3.3 VULNERABILITIES IN THE PROSECUTION OF CRIME

Achieving a low number of convictions

1. It has been found that the number of convictions for the crime of legalization of proceeds of crime and the legalization of proceeds of crime from negligence is not high, therefore there is a doubt as to whether the achievement of a low number of convictions is the consequence of the fact that the crimes are not committed in such a quantity, whether the offense is dealt with in another way (transfers), or whether there is another factor that prevents the detection and conviction of perpetrators. Another factor could be the systemic inability to obtain convictions or other systemic deficiencies or the lack of resources (personnel, financial, etc.) that could have an impact on the effectiveness of detection of crime (for more details see point VII).

2. A relatively low number of convictions can have a number of partial causes. To analyse the issue of a possible systemic shortage, it is necessary to use statistical data on the number of convicted persons available to the Ministry of Justice. As can be seen from the overviews below, from 2013 onwards, the number of persons convicted for legalization of proceeds of crime and the legalization of proceeds of crime from negligence is constantly increasing. These statistics, point to an opposite trend, i.e., to the fact that, this crime is penalized. Nevertheless, even with the use of these statistics, it is not possible to assess whether the increasing number of convictions is the result of a better outcome in the detection and prosecution of such offenses, or whether the reason is an increase in the total number of offenses committed.

Table 1: Number of persons convicted of Section 216 and Section 217 in 2013, 2014 a 2015

Year 2013	**§ 216**	
Totally convicted		30
Paragraph	1	1
	2	19
	3	9
	4	1

Year 2013	**§ 217**	
Totally convicted		15
Paragraph	1	13
	2	1
	3	1

Year 2014	**§ 216**	
Totally convicted		47
Paragraph	1	9
	2	25
	3	12
	4	1

Year 2014	**§ 217**	
Totally convicted		26
Paragraph	1	25
	2	1
	3	0

Year 2015	§ 216	
Totally convicted		57
Paragraph	1	7
	2	37
	3	13
	4	0

Year 2015	§ 217	
Totally convicted		52
Paragraph	1	47
	2	5
	3	0

3. It is also worth noting that the above statistical data show that the highest number of convictions concerning the offense of legalizing proceeds of crime is linked to a qualified factual matter under Section 216 para 2 of the Criminal Code (i.e., the offense of legalization of proceeds of crime is committed in relation to a matter of greater value or if the perpetrator obtains for himself or for some other grater benefit).

In order to assess the trend of detecting the offenses in question, it is also necessary to use statistical data on the number of persons prosecuted:

Table 2: Number of persons prosecuted for Section 216 and Section 216 and Section 217 during 2013, 2014 a 2015

Criminal offense of legalization of proceeds of crime (Section 216)	Number of prosecuted	Plus shortened preparatory proceedings
Year 2013	91 person	5 persons
Year 2014	155 persons	9 persons
Year 2015	170 persons	2 persons

Criminal offense of legalization of proceeds of crime from negligence (Section 217)	Number of prosecuted	Plus shortened preparatory proceedings
Year 2013	35 osob	5 persons
Year 2014	52 persons	11 persons
Year 2015	94 persons	7 persons

As can be seen, the number of prosecuted persons has also increased significantly. In assessing the difference between the number of persons prosecuted and the number of convictions, it is necessary to keep in mind not only the total duration of criminal proceedings but also the principle of the presumption of innocence and the related realization of the right of defence.

4. One possible cause of a low number of separate convictions for the legalization of proceeds of crime may be the fact that the financial investigation, i.e., identification, search and seizure of proceeds of crime, including laundered assets, is relatively closely related to

the criminal offense under investigation, where the financial investigation is conducted in particular to the extent that it is necessary to identify the characteristics of the facts of the predicate offence and a separate financial investigation focused solely on determining where the proceeds of the predicate offence are and who contributed to their legalization is not always thoroughly conducted, which is due, for a small part, to legislative reasons and to a greater part to practical reasons, namely the insufficient personal capacities (the need to increase the number of specialists focusing on the financial investigation) and partly by the fact that the financial investigation prolongs criminal proceedings and law enforcement authorities have a primary interest in prompt conviction of the perpetrator and focus primarily on proving guilt.

Measures:

I. On 1 January 2012, the new Act No. 418/2011 Coll., on the criminal liability of legal persons and proceedings against them entered into force. This Act regulates conditions of criminal liability of legal persons, penalties and protective measures that may be imposed on legal persons for illegal acts committed by them and the procedure in proceedings against legal persons. Until the entry into force of this law, the criminal liability of legal persons could not be based.

A legal person may be prosecuted under this Act for a number of criminal offenses, including for example the criminal act of legalization of proceeds of crime and the legalization of proceeds of crime from negligence.

II. Act No. 165/2015 Coll., amending Act No. 40/2009 Coll., Criminal Code, as amended (the Act entered into force on 1 September, 2015), responded, i.a., to requirements set out in the Evaluation Report of the Czech approved by Group of States Against Corruption (GRECO) in the third round of evaluation in spring 2011 and requirements of the Committee of Experts on the Evaluation of Anti-Money Laundering and the Financing of Terrorism (Moneyval). On the basis of Recommendation 1 of the Report of the Fourth Evaluation Visit of Moneyval, criminality of preparatory acts for certain offenses against property, namely in the crime of participation and legalization of proceeds of crime was introduced in the Czech criminal law. This change is based not only on the recommendations of the Moneyval, but also on international treaties ratified by the Czech Republic and Recommendations of the FATF.

III. Following the results of the evaluation report of the Council of the European Union on the fifth round of mutual evaluations on financial crime and financial investigations and for streamlining activities in pre-trial criminal procedures, the role of the Supreme Public Prosecutor's Office was strengthened. For securing specialization of the Public Prosecutor's Office the amendment of Decree no. 23/1994 Coll., On the Rules of Procedure of the Prosecutor's Office, the establishment of branches of some prosecutors' offices and details of actions taken by legal trainees by Decree no. 4/2014 Coll., extended the jurisdiction of the Supreme Public Prosecution also to the supervision of the observance of legality in pre-trial procedures in cases of crimes of participation pursuant to Section 214 of the Criminal Code, negligent participation under Section 215 of the Criminal Code, the legalization of proceeds of crime under Section 216 of the Criminal Code and the legalization of the proceeds of crime by negligence under Section 217 of the Criminal Code, in cases where the predicate

offense is one of the offenses supervised by prosecutors of Supreme Public Prosecutor's Office.

IV. Amendment to the criminal law by Act No. 86/2015 Coll., effective on 1 June 2015, enacted the compulsory forfeiture of the so-called direct proceeds of crime belonging to the perpetrator (i.e., things that were obtained by a crime or as remuneration for it). The stated obligation of the court to impose a penalty of forfeiture of a items pursuant to Section 70 of the Criminal Code in relation to the immediate proceeds of crime should contribute to the fact that prosecutors will propose the imposition of such a sentence and, at the same time, the proceeds will be more searched for and secured for that purpose. This amendment, following the government-approved Analysis of Enhanced Asset Management and Purchase of Assets, made a number of adjustments in the field of asset management to streamline it and reduce its financial cost, which should contribute to the effective provision of instruments and profits from which the law enforcement authorities engaged in criminal proceedings will not be discouraged by the vision of the subsequent difficulties associated with the management of the seized property.

In particular, changes have been made to extend conditions for the sale of assets secured in criminal proceedings, the unambiguous definition of the status of the asset manager secured in criminal proceedings, the administration of shareholding in a commercial corporation secured in criminal proceedings, the extension of conditions for securing claims of the injured party in criminal proceedings, enabling to secure part of assets of an accused for the purpose of forfeiture of assets, enabling to secure assets of an accused for the purpose of executing the pecuniary penalty and the compulsory forfeiture of proceeds of crime of perpetrators.

V. Currently, there is a proposal amending Act No. 40/2009 Coll., the Criminal Code, as amended and other related laws, which is expected to take effect on 1 October 2016. The proposal extends reasons for obtaining necessary banking information and information from the bookkeeping of securities and investment instruments in criminal proceedings or to order the monitoring of accounts where it is explicitly stated that such instruments may also be used to determine the nature, extent or location of items for the purpose of ensuring the execution of a criminal sanction or for the purpose of determining the financial circumstances of the accused, which makes it possible to use these instruments only for the purpose of seeking, securing and withdrawing instruments and proceeds of crime.

It also regulates the authority of law enforcement authorities to use the institute of declaration of assets for the purpose of determining the nature, extent or location of items for the purpose of securing them, for the purpose of ensuring the execution of a criminal sanction or for the purpose of determining the financial circumstances of the accused. The person whose assets are secured or a person close to this person may be invited to file the declaration of assets. The person is required to state, in the declaration of assets, to the extent that such facts are known to him/her, the data relating to the assets of the person whose assets are secured, in particular:

- A payer of remuneration from an employment relationship or a similar relationship or other income and the amount of such remuneration or other income;

- For which bank, savings bank, credit institution, electronic money institution, small-scale electronic money issuer, payment institution, small-scale payment service provider or similar foreign person, the person has accounts, amount of receivables and account numbers or other unique identifiers under the Payment System Act ,
- Debtors to whom a person have financial claims, their reason, amount and repayment term;
- An overview of immovable property and movable property, including cash, ownership or co-ownership of that person, including an indication of the share of ownership and the location of items;
- Property rights and other intangible assets owned by that person;
- Trusts that this person has established or for which he is a beneficiary.

The statement is made in writing, if the person does not submit it, it is incomplete or if the LEA has doubts about its correctness, it shall summon the person for oral questioning.

Following Article 5 of Directive 42/2014/EU, a new safeguard measure is included in the Criminal Code to secure part of assets (Section 102a of the Criminal Code), which allows for the deduction of probable proceeds from unproven crime. The prerequisites for imposing this protective measure are:

- The perpetrator has been convicted of an intentional criminal offense with an upper limit of imprisonment of at least 4 years or a designated offense;
- The perpetrator obtained or attempted to obtain criminal assets;
- Other facts have been identified by which the court considers that certain assets of the perpetrator originate in criminal activity – in particular the disproportion between the statutory income and the total property of the perpetrator during the relevant period (up to 5 years before the offense), including assets the perpetrator in the decisive period transferred to other persons; the previous conviction of the offender for a profit-generating crime; contacts with criminal persons; participation in an organized profit-oriented group; transfers of funds in principle in cash, etc.

Forfeiture of a part of assets in relation to a particular item may be imposed on a person other than the perpetrator, if this item had been transferred by the perpetrator or if that person knew of the illegal origin of such item or the unlawful purpose of its acquisition. It is also possible to seize assets acquired by the perpetrator in the matrimonial assets and assets transferred to a trust.

For the purposes of determining the conditions for imposing such safeguard measures or for the purpose of ensuring its enforcement, the amendment allows the Czech Financial Administration to request information on the amount of the tax on income of the person concerned.

The present amendment also simplifies and unifies the forfeiture institutes that are applicable to securing instruments and proceeds of crime.

VI. One possible measure is to raise awareness among LEAs of the importance of identifying, securing and withdrawing proceeds of crime. Disseminating awareness to

increase the number of convicted perpetrators and to increase the volume of forfeited assets of serious predicate offence, can be an appropriate measure to minimize impacts on identified vulnerabilities. In the framework of training for LEAs, emphasis is placed on the search, securing and withdrawal of criminal proceeds. This issue is a regular topic of training for judges, prosecutors and police authorities. E.g., at the Judicial Academy, a three-day training session was held in January 2016, concerning the search, securing and withdrawal of instruments and proceeds in criminal proceedings and the administration of assets secured in criminal proceedings.

VII. The eventual increase in the number of prosecuted persons is (with a view to the limit represented by the objective number of crimes actually committed) a matter of detecting these crimes.

The abovementioned data on the increasing number of persons prosecuted under Sections 216 and 217 of the Criminal Code are evidence of increased activity of the Czech Police in this area where the attention of the police was also paid to organized groups of perpetrators focusing on money laundering itself, without committing predicative crime. The activity of police specialists in financial investigations, which reveals not only asset values eligible to be secured in criminal proceedings but also traces leading to the legalization of proceeds of crime, can be positively evaluated.

However, the described positives revealed at the same time insufficient number of policemen specializing in economic crime within the Czech Police. The Strategic Development Document of the Police (“Concept of Development of the Czech Police up to 2020”), which will be submitted to the Czech Government in 2016, also provides for increasing the number of staff of the Corruption Detection and Financial Crime Unit and the Criminal Police and Investigation Service at Regional Directorates.

Reporting deficiencies

1. Shortcomings were found in the Ministry of Justice statistics on criminal convictions. Information on predicative crime in relation to money laundering is not reported in all cases in these statistics. The statistics also do not directly record instances of consumption.
2. The Ministry of Justice in line with the strategic document "The eJustice Development Strategy", which is expected to make significant changes to the computerization of justice in the years to come, will address the issues of reporting and statistics. It is expected that a new statistical information system will be introduced to provide top-level ministry and court management with operational data for management, unifying and centralizing statistical data throughout the justice sector and providing easy and secure access to this information. The deployment of the system is expected in the 2017-2020.
3. The evaluation of the Moneyval noted to shortcomings in completeness and accuracy of statistics on money laundering and terrorism financing. It was found, i.a., than in certain cases the perpetrator's conviction was only referred to in the statistical data sheet as a predicative (underlying) criminal offense, although in fact the perpetrator

was sentenced both for the predicative (underlying) crime and for the legalization of proceeds of crime. Following the Moneyval evaluation, the Ministry of Justice sent a letter to all presidents of regional and supreme courts requesting that information on convictions for the legalization of criminal proceeds and participation is consistently filled in the statistical data sheets.

4. In solving the issue of data reporting in the statistical systems of the Ministry of Justice, a request was made for the addition of the following categories to statistical surveys of MoJ in relation to money laundering:

   - Clear reporting of predicative crime for convictions for the legalization of proceeds of crime;
   - The value of secured, forfeited and seized assets;
   - Type of character of forfeited and seized items;
   - Data not only about the amount of financial penalties imposed in the relevant calendar year (Section 67 of the Criminal Code), but also how many of them were ordered to enforce them and what amount was obtained on the basis of voluntary reimbursement from the offender and what amount was obtained by enforcing financial penalty;
   - Data on international legal assistance in case of money laundering (requesting/receiving country, number of requests from the CR/to the CR, type of legal assistance requested, way of processing the application, duration of settlement).

These requirements should be reflected in the new system.

Measures:

I. The impacts on this vulnerability can be eliminated by streamlining statistical reporting and extending the metadata under review. The Ministry of Justice is currently preparing a new system of statistics. Therefore, the projection of some data tracking requirements is probably a matter of technical solution and acceptable level of burden on data providers.

Legalization of proceeds of crime is also committed by specialized groups of perpetrators who do not commit predicate crime

1. The current diction of Sections 216 and 217 does not presuppose that a person committing a crime of legalization of proceeds of crime or legalization of proceeds of crime by negligence must be at the same time a perpetrator of an predicate offence ("Whoever conceals the origin or otherwise attempts to substantially complicate or render impossible to establish the origin of things ... whoever allowed the commission of such an act to another person, or conspires for the purpose of committing such an act ... "). Thus the perpetrator can be anyone, including the perpetrator of the predicate offence. Therefore, if the

perpetrator of an predicate offence is different from the perpetrator of a criminal offense pursuant to Sections 216 or 217, he/she may be punished according to the existing legislation.

2. As regards activities of specialized groups, the existing Section 216 para 3 letter a) takes into account the offense of legalizing the proceeds of crime by a member of an organized group, with the offender being punished by imprisonment for two years to six years or by forfeiture of property.

3. If a specialized entity is a legal person, the law on criminal liability of legal persons and proceedings against them may also be applied by this Act as from 1 January 2012, when Act No. 418/2011 Coll., came into force. A legal person may commit offenses of participation and legalization of proceeds of crime in both deliberate and negligent forms, whereby the legal person may also be ordered to be abolished (see Section 15 et seq. of the Act), if the activity consisted wholly or predominantly in committing a criminal offense or offenses.

4. Since 1 January 2010, when Act No. 41/2009 Coll., On Amendments to Certain Acts in Connection with the Adoption of the Criminal Code, has come into force, the institute of the co-operating accused, which has been introduced into the Czech legal system in order to facilitate clarifying crimes committed by members of an organized group, in association with an organized group or in favour of an organized criminal group, can be used in criminal proceedings.

5. Establishing, participating in activities and supporting an organized criminal group is a criminal offense of participation in an organized criminal group under Section 361 of the Criminal Code. The tightening of sanctions for crimes committed in favour of an organized criminal group is dealt with in Section 108 of the Criminal Code, according to which the upper limit of the penalty for imprisonment has increased by one third and the penalty is imposed in the upper half of the penalty rate thus determined.

Measures:

I. In order to effectively uncover criminal activities of organized groups and to punish their members correctly, the law institute of the co-operating accused person (Section 178a of the Code of Criminal Procedure) was incorporated into the criminal procedure code as of 1 January 2010 as a means of ensuring the motivation of the accused – the person involved in the activities of an organized criminal group – and organized groups to cooperate with LEAs. The designation of the accused person as a co-operator may lead to his/her punishment being dropped. The amendment was made by Act No. 41/2009 Coll., On Amendments to Certain Acts in Connection with the Adoption of the Criminal Code and the provision was modified by Act No. 193/2012 Coll.

II. Since 1 January 2010, Act No. 306/2009 Coll., amending Act No. 40/2009 Coll., the Criminal Code and some other laws that tightened the punishment of crimes committed for the benefit of an organized criminal group has been effective. Since the effective date of this law it is possible that the upper limit of the penalty rate of imprisonment increased by one third (see paragraph 4 above) was over twenty years.

4.1 SUMMARY OF RISKS AND NECESSARY ADDITIONAL MEASURES

The following table summarizes the assessed risks and the necessary additional measures to mitigate them. As already described in the methodology, the ML/TF national risk assessment process implements the formulation of measures as an integral part of risk management and hence also as an integral part of the process. The formulation of the measure does not create any further process that would be arbitrarily separated from the risk assessment.

The table contains all those risks that require additional mitigation that have been described and evaluated throughout the process, regardless of the sub-process and whether or not the vulnerability component or threat component or their impact, respectively, is more relevant. Practically, with minor exceptions, it is the mutual conditioning of all three components of risk, only the proportion of their relevance may vary. At this point we no longer provide any measures (or risks) that would not come from the risk assessment process. A more comprehensive description of the risks summarized here can be found in the previous chapters. The measures can be both legislative and non-legislative and their content extends from the educational activity to the criminalization of certain actions

Given that the information in some of the previous chapters is specific and sensitive (and therefore sharing of such chapters is limited), the description of risks and measures in the following table is only general. The attributed risk rate of risks presented here is expressed on the scale: serious, moderate and not significant[44]. In line with the FATF methodology, risk mitigation should be undertaken, depending on its seriousness. I.e., the more serious the risk is, the sooner it needs to be mitigated. The ranking of risks and corresponding measures in the table is based on the order of chapters in this Report, or of sub-processes, from which risks and the follow-up measures originated.

[44] We do not mention low risks here as there is no need for additional measures to mitigate them. Rows with serious risks are marked in red, those with moderate orange and those with not significant yellow.

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Neccesity to set the periodicity of the NRA process	Methodology and Selected Procedures	1.4	Moderate	To set the periodicity of the NRA process	Non-legislative	FAU and other authorities concerned	Carry out the 2nd round of the NRA process and submit a Report thereon to the Government not later than 31. 12. 2020; or update relevant parts of the NRA with respect to the development of ML/TF risks without delay.	Prevention / analysis, investigation and prosecution
Time consuming access of authorities concerned to information (on account holders and on persons entitled to act on behalf of the account holder) and risk of misuse of information by requested institutions	Assessment of Threats	2.1	Moderate	Establishment of the Central Register of Accounts	Legislative / Non-legislative	Legislation: FAU; Implementation: CNB	Act No. 300/2016 Coll. Fully effective from 1. 1. 2018	Prevention / analysis, investigation and prosecution
Selected typologies of predicate offence and subsequent money laundering techniques described in the Chapter on Threats	Assessment of Threats	2.1	Serious	Incorporate and consistently apply defined risk factors and suspicious indicators	Part of CDD; already in the current AML Act	Obliged entities	Immediately	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Selected typologies of predicate offence and subsequent ML techniques described in the Chapter on Threats	Assessment of Threats	2.1	Moderate	Re-consider the exemption; simplified CDD in case of selected financial institutions, respectively.	Legislative	FAU	Next amendment to the AML Act	Prevention
Misuse of cash in selected typologies of predicate offence and subsequent ML techniques described in the Chapter on Threats	Assessment of Threats	2.1	Serious	Consistently apply CDD and reflect the factor of cash in detection of suspicious transactions	Part of CDD; already in the current AML Act	Obliged entities	Immediately	Prevention
Misuse of mortgage loans and other residential real estate loans in selected typologies of predicate offence and subsequent ML techniques described in the Chapter on Threats	Assessment of Threats	2.1	Serious	Categorize mortage loans and other residential real estate loans as risk products and set appropriate CDD	Part of risk assessment and subsequent proportionate CDD; already in the current AML Act	Obliged entities	Immediately	Prevention
Opaque ownership structure	Assessment of Threats	2.1	Serious	Introduce the obligation of LPs and trusts to know BOs	Legislative	FAU	Amendment to the AML Act; supposedly effective from 1. 1. 2017	Prevention
Opaque ownership structure	Assessment of Threats	2.1	Serious	Establish a register of beneficial owners	Legislative	MoJ	Amendment of Act No. 304/2013 Coll., on Public Registries; supposedly effective from 1. 1. 2018	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Inadequate registration of trusts	Assessment of Threats	2.1	Serious	Establish a register of trusts	Legislative	MoJ	Proposal of amendment to the Civil Code and other acts; currently in the Chamber of Deputies	Prevention
Intra-communitarian transport of cash	Assessment of Threats	2.1	Moderate	Consider the introduction of control and monitoring of intra-communitarian transports of cash	Non-legislative: inter-departmental working group and analysis of the need to introduce intra-communitarian cash transport controls	MoI	Preparatory work was carried out within the inter-departmental working group coordinated by the MoI	Prevention
Risk of involvement of insiders form the private sector	Assessment of Threats	2.1	Serious	Incorporate into internal risk management systems	Preventive risk management systems of obliged entities	Obliged entities	Already implemented	Prevention
Risk of involvement of insiders form the private sector	Assessment of Threats	2.1	Serious	Criminalse such practice	Legislative	MoJ	Already in the current Criminal Code	Analysis, investigation and prosecution
Risk of involvement of insiders form the private sector	Assessment of Threats	2.1	Serious	Take action within the state anti-corruption policy	Legislative	State authorities	Already implemented	Analysis, investigation and prosecution

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Insuficient criminalisation of TF	Assessment of Threats	2.1	Serious	Criminalise TF in the Criminal Code	Legislative	MoJ	Amendment to the Criminal Code submitted to the Chamber of Deputies	Analysis, investigation and prosecution
Insuficient knowledge of ML/TF risks and their management	Assessment of Threats/Legal and Advisory Professions	2.1/ 3.1.10	Serious	Carry out sectoral ML/TF risk assessment	Non-legislative: recommendation	SRBs of legal and advisory professions	Continuously	Prevention
Insuficient knowledge of ML/TF risks and their management	Assessment of Threats/Legal and Advisory Professions	2.1/ 3.1.10	Serious	Raise awareness on AML/CFT prevention	Non-legislative: awareness raising, guidance	SRBs	Immediately	Prevention
Insuficient knowledge of ML/TF risks and their management	Assessment of Threats/Legal and Advisory Professions	2.1/ 3.1.10	Serious	Strenghten dialog with SRBs and raise awareness of AML/CFT prevention	Non-legislative: awareness raising, guidance	FAU	Continuously	Prevention
Insufficient supervision	Assessment of Threats/Legal and Advisory Professions	2.1/ 3.1.10	Serious	Strenghten supervision and level playing field (“best cannot be beaten”)	Non-legislative: supervision	SRBs of legal and advisory professions	Continuously	Prevention
Insufficient supervision	Assessment of Threats/Legal and Advisory Professions	2.1/ 3.1.10	Serious	Unambiguous obligation of SRBs to perform supervision and report thereon to the FAU	Legislative	FAU	Next amendment to the AML Act	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Insufficient supervision	Assessment of Threats/Legal and Advisory Professions	2.1/ 3.1.10	Serious	Use existing tools in Sections 36 and 37 of the AML Act and selected procedures under the AML Act	Non-legislative	FAU	Continuously	Prevention
Implementation of the requirement in FATF R.28b	Assessment of Threats/Legal and Advisory Professions	2.1/ 3.1.10	Moderate	Iniciate dialog with sectoral regulators	Primarily non-legislative	FAU	After approval of the NRA Report	Prevention
Risk of misuse of corporate structures and trusts (on the side of service providers; for other components of this risk and mitigation measures see above)	Assessment of Threats/ Company Service Providers and Trusts	2.1/ 3.1.11	Moderate	Continue of supervision of trust and company service providers	Non-legislative: supervision	FAU/GFD	Already implemented	Prevention
Risk of misuse of alternative means of identification	Assessment of Threats/ Credit and Other Financial Institutions	2.1/ 3.1.1 - 7	Serious	Consistently apply additional measures as described in the Chapter on Credit Institutions	Non-legislative	Obliged entities, in particular credit and other financial institutions	Immediately	Prevention
Risk of misuse of alternative means of identification	Assessment of Threats/ Credit and Other Financial Institutions	2.1/ 3.1.1 - 7	Moderate	Consider appropriate actions: legislative or explanatory statement on risk mitigation	Legislative	FAU	Next amendment to the AML Act	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Structuring of cash deposits	Assessment of Threats/ Credit and Other Financial Institutions	2.1/ 3.1.1 - 7	Serious	Implement adequate additional measures to mitigate this risk	Non-legislative	Obliged entities, in particular credit and other financial institutions	Immediately	Prevention
Abuse of real estate trade	Assessment of Threats/Threat Analysis/ Real Estate Trade	2.1/ 5.5/ 3.1.9	Serious	Incorporate and consistently apply provided suspicious indicators	Part of CDD, already in the current AML Act	Credit institions and real estate agencies	Immediately	Prevention
New threats of TF	Identification and Assessment of Vulnerabilities in the Private Sector	3.1	Serious	Incorporation of other suspicious indicators on TF	Non-legislative	Obliged entities	Immediately	Prevention
Absence of ML/TF risk assessment of certain obliged entities	Identification and Assessment of Vulnerabilities in the Private Sector	3.1	Currently not serious	Carry out ML/TF risk assessment	Legislative	Obliged entities	In connection with the entry into force of the Amended AML Act	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Partial deficiencies in risk management of certain obliged entities who have already processed their risk assessments (e.g., mixing ML/TF risks with other risks or lacking justification of low risk in simplified CCD)	Identification and Assessment of Vulnerabilities in the Private Sector	3.1	Currently not serious	Consistent application of the *comply or explain* principle	Legislative	Obliged entities, in particular credit and other financial institutions	In connection with the entry into force of the Amended AML Act	Prevention
Non-standard transactions executed outside regulated markets, cash operations, transactions in paper securities, non-cash investments by investors	Assesment of Vulnerabilities in the Fund Investment Sector (investment companies and self-managed investment funds)	3.1.4	Moderate	Set up an effective management and control system; manage the conflict of interest	Risk identification and management; focus on risks associated with the fund's investment policy and investor typology (in particular, FKI)	Obliged entities (investment companies and self-managed investment funds)	Continuously (already in the current legislation)	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Non-standard transactions executed outside regulated markets, cash operations, transactions in certificated securities, non-cash investments by investors	Assesment of Vulnerabilities in the Fund Investment Sector (investment companies and self-managed investment funds)	3.1.4	Moderate	Control compliance with legal and internal regulations	Perform supervisory and control activities	CNB (sectoral and AML regulations) and FAU (AML regulations)	Continuously (already implemented, enshrined in the current legislation)	Prevention
Transactions executed outside regulated markets, cash operations, securities transactions, high frequency of transactions or short-term transactions with certain investement tools	Assessment of Vulnerabilities of Securities Traders	3.1.3	Moderate	Set up a robust management and control system	Risk identification and management, internal control, consistent CDD, categorization of customers and setting of measures in relation to individual categories, transaction monitoring	Obliged entities (securities traders)	Continuously (already in the current legislation)	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Transactions executed outside regulated markets, cash operations, securities transactions, high frequency of transactions or short-term transactions with certain investement tools	Assessment of Vulnerabilities of Securities Traders	3.1.3	Moderate	Control compliance with legal and internal regulations	Perform supervisory and control activities	CNB (sectoral and AML regulations) a FAU (AML regulations)	Continuously (already implemented, enshrined in the current legislation)	Prevention
Possible accumulation of small payments	Assessment of Vulnerabilities of E-Money Issuers (EMI a VEMPR)	3.1.5	Currently not serious	Set up a management and control system	Consistent monitoring of executed transactions and business relationships (the role of so-called agregators)	Obliged entities (entities on the market with payment services)	Continuously (already in the current legislation)	Prevention
Cash payment transactions, risk of involvement of agents/sales representatives (money remittance) cash-less transfers	Assessment of Vulnerabilities of Payment Service Providers (payment institutions and small-scale payment service providers)	3.1.5	Serious (money remittance)	Set up a management and control system	CDD, transaction monitoring, systematic control of agents/sales representatives	Obliged entities (entities on the market with payment services)	Continuously (already in the current legislation)	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Cash payment transactions, risk of involvement of agents/sales representatives (money remittance) cash-less transfers	Assessment of Vulnerabilities of Payment Service Providers (payment institutions and small-scale payment service providers)	3.1.5	Serious (money remittance)	Perform supervisory and control activities	Control compliance with legal and internal regulations	a) CNB (sectoral and AML regulations) and b) FAU (AML regulations	Continuously (already implemented; enshrined in the current legislation)	Prevention
Cash payment transactions, risk of involvement of agents/sales representatives (money remittance) cash-less transfers	Assessment of Vulnerabilities of Payment Service Providers (payment institutions and small-scale payment service providers)	3.1.5	Moderate (cash-less transfers and cash payment transactions)	Set up a management and control system	CDD, transaction monitoring, systemetic control of agents/sales representatives	Obliged entities (entities on the market with payment services)	Continuously (already in the current legislation)	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Cash payment transactions, risk of involvement of agents/sales representatives (money remittance) cash-less transfers	Assessment of Vulnerabilities of Payment Service Providers (payment institutions and small-scale payment service providers)	3.1.5	Moderate (cash-less transfers and cash payment transactions)	Perform supervisory and control activities	Control compliance with legal and internal regulations	a) CNB (sectoral and AML regulations) and b) FAU (AML regulations	Continuously (already implemented; enshrined in the current legislation)	Prevention
Two groups of risks - from exchange service providers (overstating volumes of executed exchange transaction) and from customers (structuring transactions)	Assessment of Vulnerabilities of Bureaus-de-Change Services	3.1.7	Serious	Verify the accuracy of the reporting obligation, issuing transaction documents, mystery shopping, controlling performance of CDD	Perform supervisory and control activities	CNB (all) and FAU (without controlling reporting obligation)	Continuously (already implemented; enshrined in the current legislation)	Prevention
Two groups of risks - from exchange service providers (overstating volumes of executed exchange transaction) and from customers (structuring transactions)	Assessment of Vulnerabilities of Bureaus-de-Change Services	3.1.7	Serious	Identify, assess and manage risks	Consistent performance of CDD	Obliged entities (bureaus-de-change)	Continuously (already in the current legislation)	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Large number of obliged entities and their considerable variety of types	Supervision by the FAU	3.2.1.1	Moderate	Continue to cover the entire spectrum of obliged entities, in the application of RBA and outputs from the NRA and in cooperation with other competent authorities	Non-legislative: supervision	FAU	Already implemented	Prevention
Large number of obliged entities and their considerable variety of types	Supervision by the CNB	3.2.2	Moderate	Continue with effective supervision while using system of comprehensive risk assessment of financial institutions and outputs of the NRA	Non-legislative: supervision	CNB	Already implemented	Prevention
Large number of obliged entities	Supervision by the CTIA	3.2.3	Moderate	Perform supervision of both types of obliged entities (i.e., traders in items of cultural heritage and brokers thereof; and traders in used goods and brokers thereof) with respect to ML and TF risks	Non-legislative: supervision	CTIA	Continuously	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Risk of misuse of postal and freight transport for cash transfers	Cross-Border Transport of Cash	3.2.5.1	Serious	Set reporting obligations for senders or recipients of consignments and exercise control over the fulfillment of this obligation	Legislative/ Non-legislative	Legislation: FAU Supervision: CACR	Already implemented	Prevention
Risk of structuring of transported funds	Cross-Border Transport of Cash	3.2.5.1	Serious	Set reporting obligations for tranports in the course of twelf consecutive months	Legislative/ Non-legislative	Legislation: FAU Supervision: CACR	Already implemented	Prevention
Structuring among multiple NPs	Cross-Border Transport of Cash	3.2.5.1	Moderate	Consider possibilities of effective mitigation of the risk	Primarily Non-legislative	Inter-departmental working group coordinated by the MoI; its activity has been terminated	Subsequent work will be the subject of negotiations among the authorities concerned	Prevention
Abuse of intra-communitarian transports of cash	Cross-Border Transport of Cash	3.2.5.1	Moderate	Consider possibilities of effective mitigation of the risk	Primarily Non-legislative (analysis of the need to introduce control of intra-communitarian transports of cash)	Inter-departmental working group coordinated by the MoI; its activity has been terminated	Subsequent work will be the subject of negotiations among the authorities concerned	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Necessity to share information on cross-border transports of cash	Cross-Border Transport of Cash	3.2.5.1	Serious	Sharing of information with the FAU and its subsequent use	Non-legislative: sharing of information	FAU and CACR	Already implemented	Analysis, investigation, prosecution
Corruption environment	Corruption as a Vulnerability	3.3.1	Serious	Uncover unreported income	Legislative	MoF	The Act on the Proof of Origin of Assets was promulgated in the Collection of Laws under No. 321/2016 Coll.	Prevention/ Analysis, investigation, prosecution
Corruption environment	Corruption as a Vulnerability	3.3.1	Serious	Strenghten the transparet functioning of political parties	Legislative	MoI/KML	Amendment to Act No. 424/1991 Coll., on the Association of Political Parties was promulgated in the Collection of Laws under No. 302/2016 Coll.	Prevention
Corruption environment	Corruption as a Vulnerability	3.3.1	Serious	Establish a register of contracts and ensure the economic management of the state property	Legislative	MoI	Act No. 340/2015 Coll. is already effective	Prevention
Corruption environment	Corruption as a Vulnerability	3.3.1	Serious	Introduce the obligation to report on activities that could create a conflict of interest	Legislative/ Non-legislative	Legislation: KML/MoJ Implementation: MoJ	Proposal of amdnedment of Act No. 159/2006 Coll. was adopted by the Parliament.	Prevention
Corruption environment	Corruption as a Vulnerability	3.3.1	Serious	Strengthen transparency in public procurement	Legislative	Ministry of Regional Development	Act No. 134/2016 effective from 1. 10. 2016	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Corruption environment	Corruption as a Vulnerability	3.3.1	Serious	Firstly, cover domestic PEPs; secondly, include both obliged entities and virtual currency service providers with; thirdly, reduce a cash payment limit; fourthly, strengthen the transparency of LPs and trusts	Legislative	FAU	Amendment to the AML Act adopted by the Parliament	Prevention
Corruption environment	Corruption as a Vulnerability	3.3.1	Serious	Extend seizure powers	Legislative	MoJ	Proposal of amendment of Act is currently in the Chamber of Deputies	Analysis, investigation, prosecution
Corruption environment	Corruption as a Vulnerability	3.3.1	Serious	Re-adapt the issue of Public Prosecution Office in order to minimize the risk of undesirable influence; establish a new Specialized Public Prosecution Office	Legislative	MoJ	Proposel is being discussed in the Chamber of Deputies	Analysis, investigation, prosecution

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Unavailability of certain information on NPOs	Vulnerability of NPOs	3.3.2	Serious	Extend the scope of publicly available information on all non-church NPOs (information on church legal persons is already publicly available)	Legislative	MoJ	Amendment to the Act No. 304/2013 Coll. is already effective	Prevention
Risk of abuse of NPOs to TF (and other criminal activities)	Vulnerability of NPOs	3.3.2	Serious	Prohibit the establishment of entities aiming to violate the law and decide on their cancellation and liquidation, resp.	Legislative	MoJ (Civil Code)/ Ministry of Culture (Act on Churches)	Relevant provisions of the Civil Code and the Act on Churches are already effective	Prevention
Insufficient transparency	Vulnerability of NPOs	3.3.2	Serious	Support and promote transparentncy	Non-legislative: eduction and dialogue	RVNNO a Ministry of Foreign Affairs	Already implemented	Prevention
Insufficient provability of record-keeping	Vulnerability of NPOs	3.3.2	Serious	Promote and controle provable record-keeping	Legislative/ Non-legislative	Legislation: MoF, MoI Supervision: GFD, competent administrative authorities according to the Act on Public Collections	Already implemented, enshrined in the current legislation (Act on Accounting, Act on Income Taxes, Act on Tax Administration, Act on Public Collections)	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Risk of abuse of NPOs to TF	Vulnerability of NPOs	3.3.2	Serious	Collect information and investigate suspicion	Non-legislative	NOCA	Already implemented, enshrined in the current legislation	Investigation, prosecution
Risk of abuse of NPOs to TF	Vulnerability of NPOs	3.3.2	Serious	First, defining a vulnerable segment of NPOs; secondly, to consider applying additional risk mitigation measures; thirdly, strengthen cooperation and information sharing	Primarily non-legislative	Inter-departmental working group coordinated by the MoI	Working group will iniciate its work befor the end of 2016	Prevention/ Analysis, investigation, prosecution
Low number of convictions	Vulnerabilities in the Prosecution of ML/TF	3.3.3	Serious	Introduce criminal liability of legal persons	Legislative	MoJ	Act No. 418/2011 Coll. is already effecitve	Analysis, investigation, prosecution
Low number of convictions	Vulnerabilities in the Prosecution of ML/TF	3.3.3	Serious	Criminalise preparation for certain offenses	Legislative	MoJ	Amendment to the Criminal Code is already effective – Act No. 165/2015 Coll.	Analysis, investigation, prosecution
Low number of convictions	Vulnerabilities in the Prosecution of ML/TF	3.3.3	Serious	Strenghten the role of Supreme Public Prosecutor's Office	Legislative	MoJ	Amendment to the Decree No. 23/1994 Coll. is already effective – No. 226/2016 Coll.	Analysis, investigation, prosecution

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Low number of convictions	Vulnerabilities in the Prosecution of ML/TF	3.3.3	Serious	Introduce mandatory forfeiture of so-called direct proceeds from crime	Legislative	MoJ	Amendment to criminal regulations is already effective – Act No. 86/2015 Coll.	Analysis, investigation, prosecution
Low number of convictions	Vulnerabilities in the Prosecution of ML/TF	3.3.3	Serious	Modify the LEAs authorization to use certain financial information or the newly established Assets Declaration; introduce a new safeguard measure of confiscation of assets	Legislative	MoJ	Proposal of amendment of criminal regulations is currently discussed in the Chamber of Deputies	Analysis, investigation, prosecution
Low number of convictions	Vulnerabilities in the Prosecution of ML/TF	3.3.3	Serious	Raising awareness of LEAs and dialoge among LEAs	Non-legislative: dialogue, education	MoJ	Continuously	Analysis, investigation, prosecution
Legalisation by third parties	Vulnerabilities in the Prosecution of ML/TF	3.3.3	Serious	Incorporation of co-operating accused institute	Legislative	MoJ	Amendment of Criminal Code is already effective – Act No. 41/2009 Coll.	Analysis, investigation, prosecution
Legalisation by third parties	Vulnerabilities in the Prosecution of ML/TF	3.3.3	Serious	Tighten punishment for perpetrators of crimes committed in the benefit of an organized group	Legislative	MoJ	Amnedment of Criminal Code is already effective	Analysis, investigation, prosecution

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Deficiencies in reporting convictions for crimes	Vulnerabilities in the Prosecution of ML/TF and the Analysis of the PPO	3.3.3/ 5.10	Moderate	Firstly, to introduce clear reporting of predicative crime in a conviction for legalization; secondly, to report volumes and types of the seized, forfeited and confiscated assets; thirdly, data on the pecuniary penalties, their possible recovery; and fourthly, record data on international legal aid, etc.	Non-legislative: implementation of "The eJustice Development Strategy"	MoJ	System deployment is anticipated from 2017 to 2020	Analysis, investigation, prosecution
Insufficient prevention of trusts	Threat Analysis	5.5	Serious	Also include trust service providers under the Czech law among obliged entities (trusts under foreign law already included)	Legislative	FAU	Amendment to the AML Act with expected effectivity from 1. 1. 2017	Prevention
Insufficient prevention of virtual currencies	Threat Analysis	5.5	Serious	Incorporate traders with virtual currencies among obliged entities	Legislative	FAU	Amendment to the AML Act with expected effectivity from 1. 1. 2017	Prevention

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
Insufficient prevention of gambling	Threat Analysis/ Gambling Operators	5.1/ 3.1.8	Serious	Incorporate also other gambling operators among obliged entities	Legislative	FAU	Amendment to the AML Act with expected effectivity from 1. 1. 2017	Prevention
Need to specialize on individual types of crime	Analysis of the PPO	5.10	Serious	Enhance specialization of public prosecutors on terrorist acts	Legislative	MoJ/PPO	Amendment to Decree of No. 23/1994 Coll. is already effictive – No. 226/2016 Coll.	Analysis, investigation, prosecution
Need to specialize on individual types of crime	Analysis of the PPO	5.10	Serious	Enhance specialization of public prosecutors on economic and property crime	Legislative	PPO	Corresponding amemdment of the Model organizational code in place already	Analysis, investigation, prosecution
Need to draw proceeds	Analysis of the PPO	5.10	Serious	Establish a network of public prosecutors specialized in securing proceeds of crime	Non-legislative: organizational	PPO	Already implemented	Analysis, investigation, prosecution

Short Description of the Risk	Initial Source of Identification: Reference to a sub-process	No. of Chapter in the Report	Assessment of Seriousness: (serious – moderate – currently not serious)	Short Description of measures	Type of Measure	Implementor	Date of Implementation	Location of the measure in the AML/CFT system: (prevention – analysis – investigation – prosecution)
FAU's failure to notify regional PPO on criminal complaints with regional jurisdiction	Analysis of the PPO	5.10	Moderate	Letting the PPO know about filed criminal complaints from the begining of the criminal procedure	Non-legislative: negotiation and organization: the purpose of negotiations will be to assess the possibility of re-introduction of such practice, particularly with regard to its feasibility	PPO and FAU	After adoption of the NRA Report by the Government	Analysis, investigation, prosecution
Insufficient legal regulation of data requests by the PPO in pre-trial procedure	Analysis of the PPO	5.10	Serious	Strengthen the legal basis for conducting financial investigations and detection of proceeds already in the pre-trial procedure	Legislative	FAU	Amendment to the Criminal Procedure Code in relation to the adoption of Act on Central Register of Accounts	Analysis, investigation, prosecution
Vulnerable types of obliged entities	Merged expert assessment of types of obliged entities in terms of their exposure to threats and the residual vulnerability	5.3/ 5.4	Moderate	Apply RBA in supervision	Non-legislative	Supervisory and control authorities: FAU, CNB, gambling supervisors, CTIA and SRBs	Continuously	Prevention

4.2 SUMMARY OF MOST IMPORTANT CONCLUSIONS

At this point, the most important conclusions are summed up.[45] We abstain from all the detailed analyses, the collected specific data and the expert assessments that preceded and are inevitably based on them.

Laundering techniques are clearly conditioned by the typology of predicate crimes. The most prominent threat identified in the ML/TF risk assessment, in terms of its consequences, is in particular tax crime and related laundering techniques, followed by other underlying criminal offenses, including corruption and related crimes and related laundering techniques. An extremely serious, but currently not detected threat is posed by a threat of terrorism financing. Fraud, phishing and subsequent laundering techniques are very likely to happen.

The highest degree of residual vulnerability (high exposure to threats in relation to the low level of currently enforced measures) among obliged entities represents legal and advisory professions as well as some gambling operators.

The mitigation measures resulting from the national risk assessment are both legislative and non-legislative. They are also involved in the areas of prevention, analysis, investigation and prosecution and are listed in their entirety in the previous chapter. These measures include, e.g., strengthening the ML/TF risk management in particularly vulnerable sectors, introducing measures to effectively prosecute ML, introduce changes in reporting prosecution of criminal offenses, systematic revision of certain provisions of the AML Act in the light of a dynamic risk-based approach, Implementation of the new FATF Recommendation 8.

The national ML/TF risk assessment process will need to be repeated periodically to respond to the development of identified, assessed and mitigated risks.

[45] These are only the most significant conclusions. Each subprocess has its own conclusions.

5 ANNEXESS

5.1 NUMBER OF STRS IN 2010 – 2015

Years	2010	2011	2012	2013	2014	2015
Banks	1476	1419	1589	1940	2206	1963
Building and Loan Associations	N/A	39	41	15	16	22
Credit Unions	N/A	23	17	55	32	34
Securities Traders	N/A	8	8	24	26	31
Pension Funds	N/A	4	4	1	1	5
Money Remitters	N/A	199	185	183	226	198
Leasing Companies	N/A	N/A	N/A	N/A	N/A	1
Insurance Companies	N/A	28	30	35	38	31
Bureaus de Change	N/A	16	16	29	13	26
Gambling	N/A	N/A	N/A	N/A	N/A	1
Legal and Consultancy Professions	N/A	6	7	2	19	13
Others	411	228	294	437	546	583
International STRs	N/A	N/A	N/A	N/A	69	55

Number of Criminal Complaints Compared to STRs

Year	2010	2011	2012	2013	2014	2015
Filed Criminal Complaints	296	256	429	547	680	514
Total Number of STRs	1887	1970	2191	2721	3192	2963
Secured Value	0,287 mld. CZK	0,808 mld. CZK	1,005 mld. CZK	3,003 mld. CZK	2,182 mld. CZK	5,542 mld. CZK

5.2 THREAT ASSESSMENT

Expert assessment of threats for the purpose of the national ML/TF risk assessment: experts from authorities concerned ranked ML/FT threats according to this aspect	**Level**
Ranked in descending order in terms of seriousness (most serious at the top)	**In line with FATF Methodology**
Threats: major types of predicate crime with subsequent money laundring and terrorist financing	**high / moderate / low**
Tax crimes and subsequent laundering	high
Corruption and subsequent laundering	high
Public procurement (machinations) and subsequent laundering	high
Subvention fraud and subsequent laundering	high
Terrorist financing	high
Breach of duty in administration of property of another and subsequent laundering	moderate
Fraud + phishing and subsequent laundering	moderate
Drug crime and subsequent laundering	moderate
Laundering of foreign proceeds	low

Expert assessment of threats for the purpose of the national ML/TF risk assessment: experts from authorities concerned ranked ML/FT threats according to this aspect	**Level**
Ranked in descending order in terms of frequency (most frequent at the top)	**In line with FATF Methodology**
Threats: major types of predicate crime with subsequent money laundring and terrorist financing	**High / moderate / low**
Tax crime and subsequent laundering	high
Fraud + phishing and subsequent laundering	high
Corruption and subsequent laundering	moderate
Subvention fraud and subsequent laundering	moderate
Public procurement (machinations) and subsequent laundering	moderate
Breach of duty in administration of property of another and subsequent laundering	moderate
Laundering foreign proceeds	moderate
Drug crime and subsequent laundering	low
Terrorist financing	low

Expert assessment of threats for the purpose of the national ML/TF risk assessment: experts from authorities concerned ranked ML/FT threats according to this aspect	**Level**
Ranked in descending order according to the merged aspects of seriousness of consequences: dangerousness, damage to public interest, organization, difficulties in detection, etc.	**In line with FATF Methodology**
Threats: major types of predicate crime with subsequent money laundring and terrorist financing	**high / moderate / low**
Tax crime and subsequent laundering	high
Terrorist financing	high
Corruption and subsequent laundering	high
Drug crime and subsequent laundering	high
Public procurement (machinations) and subsequent laundering	moderate
Subvention fraud and subsequent laundering	moderate
Laundering of foreign proceeds	low
Fraud + phishing and subsequent laundering	low
Breach of duty in administration of property of another and subsequent laundering	low

5.7 POLICE STATISTICS

Public – the content is in a separate Excel file

5.8 STATISTICS OF OF PROSECUTED CRIMINAL ACTIVITIES

Public – the content is in a separate Excel file

5.10 ANALYSIS OF THE PPO

Public – the content is in a separate Word file

All the public Annexes are available on the Czech FIU website: http://www.financnianalytickyurad.cz/hodnoceni-rizik/narodni-hodnoceni-rizik.html