FATF • GAFI

Financial Action Task Force Groupe d’action financière

FATF Guidance Document

Best Practices Paper

Best Practices on Trade Based Money Laundering

20 June 2008

Please note that this document refers to the FATF Recommendations as last updated and published in October 2004, and does not yet take into account the 2012 revision of the FATF Recommendations.

See www.fatf-gafi.org/recommendations for the 2012 FATF Recommendations, including the conversion table from the old Recommendation to the new FATF Recommendation.

BEST PRACTICES PAPER ON TRADE BASED MONEY LAUNDERING

Money laundering and terrorist financing through the trade system

Introduction

1. The Financial Action Task Force (FATF) has recognised misuse of the trade system as one of the main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy. As the anti-money laundering (AML) and counter-terrorist financing (CFT) standards that have been applied to other money laundering techniques have become increasingly effective, such abuse of the trade system is expected to become increasingly attractive. However, currently, many customs agencies, law enforcement agencies, financial intelligence units (FIU), tax authorities and banking supervisors (*i.e.* competent authorities) appear less capable of identifying and combating trade-based money laundering than they are in dealing with other forms of money laundering and terrorist financing.

2. The objective of this best practices paper is to improve the ability of competent authorities to collect and effectively utilise trade data, both domestically and internationally, for the purpose of detecting in a risk-based manner and investigating money laundering (ML) and terrorist financing (TF) through the trade system. The FATF will continue to explore vulnerabilities in the trade system, including those related to trade finance, with a view to identifying other measures that could be considered in combating illicit use of the trade system.

Statement of the problem

3. The FATF typologies studies indicate that criminal organisations and terrorist groups are exploiting vulnerabilities in the international trade system to move value for illegal purposes. A number of specific money laundering cases were identified which involved the proceeds from various types of predicate offences to include, but not limited to, illicit trafficking in narcotic drugs, illicit trafficking in stolen or other goods, corruption and bribery, fraud, counterfeiting/piracy of products and smuggling. The most basic schemes involve fraudulent trade practices such as: over- and under-invoicing of goods and services, multiple invoicing of goods and services, over- and under-shipments of goods and services, and falsely describing goods and services. More complicated schemes integrate these fraudulent practices into a complex web of transactions and movements of goods.[1] Inherent vulnerabilities in the international trade system, including the enormous volume of trade flows, which obscures individual transactions, provide abundant opportunity for criminal organisations and terrorist groups to transfer value across borders.

Definitions

4. For the purposes of this best practices paper, the following definitions apply.

5. The term *trade-based money laundering and terrorist financing (TBML/FT)* refers to the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origins or finance their activities. Examples of how TBML/FT may be carried out

[1] Some examples may include moving value through the financial system (*e.g.* using cheques or wire transfers), the use of front companies, the physical movement of banknotes (*e.g.* using cash couriers), and concealing bulk cash in cargo.

include, but are not limited to: misrepresentation of the price, quantity or quality of imports or exports; and money laundering through fictitious trade activities and/or through front companies.

6. The term *trade data* refers to whatever information a jurisdiction collects, by paper or electronically, on its import-export forms or supporting documentation.[2] For example, such information usually includes a description of the goods being imported or exported, their quantity, value, weight, customs or tariff code number, the mode of transportation by which the goods are being imported or exported, and/or the name and address of the exporter (consignor), importer (consignee), and shipping company. In some cases, financial or banking data is also collected.

7. The term *trade authorities* refers to the authorities who are responsible for collecting, analysing and/or storing trade data.

8. The term *investigative authorities* refers to the competent authorities who are responsible for investigating money laundering, terrorist financing and/or the underlying predicate offence (*e.g.* customs fraud, smuggling, narcotics trafficking).[3]

9. The term *trade finance* refers to the financial component of an international trade transaction (*i.e.* managing the payment for goods and related services being imported or exported). Trade finance activities may involve, among other things, managing payments for open account trading, or issuing letters of credit, standby letters of credit and guarantees.

10. The term *trader* refers to anyone who facilitates the exchange of goods and related services across national borders, international boundaries or territories. This would also include a corporation or other business unit organised and operated principally for the purpose of importing or exporting goods and services (*e.g.* import/export companies).

Capacity building and awareness raising

11. A review of the current practices of various jurisdictions shows that there is need for a stronger focus on training programs for competent authorities to enhance their ability to identify TBML/FT techniques. Consequently, a basic principle guiding the establishment of these best practices is that, in order to raise awareness and build expertise to combat TBML/FT, countries could agree to incorporate TBML/FT into existing training programs on AML/CFT. Such programs could include training to relevant law enforcement agencies concerning the existence and relevance of financial and trade data to assist in the identification of TBML/FT. Considering the challenges that may face low capacity countries in providing the training consistent with this guidance, technical assistance providers could consider incorporating TBML/FT into existing technical assistance activities.

12. Consistent with this basic principle, countries are encouraged to provide training on TBML/FT techniques to the staff of trade authorities, investigative authorities, customs agencies, tax authorities, the financial intelligence unit, prosecutorial authorities, banking supervisors and any other authorities that the country identifies as being relevant to the fight against TBML/FT (*e.g.* specialised units such as Trade Transparency Units). This training may be incorporated into existing training programmes on AML/CFT or, where no such programmes are in place, on a stand-alone basis. Countries can leverage existing expertise by developing TBML/FT training programmes in collaboration with authorities that already have

[2] The collection, use and sharing of trade data is subject to international agreements agreed between two or more countries.

[3.] In some cases, customs autorities will not have the responsibility or authority to conduct such investigations.

related experience (*e.g.* cases involving customs fraud, VAT fraud-related money laundering, black market peso exchanges, tax and excise offences may also involve a TBML/FT component). The participation of foreign experts and counterparts in such training is also useful, given the global nature of TBML/FT.

13. It is best practice in this area to tailor training programmes to meet the specific requirements and needs of different authorities. For example, financial and trade data analysis is a useful tool for identifying trade anomalies, which may lead to the investigation and prosecution of TBML/FT cases. Consequently, training programmes for analytical and investigative authorities could include a focus on the existence and relevance of financial and trade data to crime targeting, and techniques for conducting such analysis. Such techniques may include:

a) Comparing domestic and foreign import/export data to detect discrepancies in the Harmonized Tariff Schedule, country of origin, manufacturer, importer/exporter, ultimate consignee, broker, unit price, commodity activity by time period, and port of import/export.

b) Analysing financial information collected by the FIU to identify patterns of activity involving the importation/exportation of currency, deposits of currency in financial institutions, reports of suspicious financial activities, and the identity of parties to these transactions.

c) Examining cargo movements through the comparison of import/export documentation between two counties to verify that the data reported to one country's authorities matches the data reported to the other country's authorities.

d) Examining domestic import data with an automated technique, such as Unit Price Analysis, to compare the average unit price for a particular commodity and identify traders who are importing commodities at a substantially higher or lower price than the world market.

e) Comparing information such as the origin, description and value of the goods, particulars of the consignee and consignor, and the route of shipment with intelligence information in existing databases to detect any irregularities, targets or risk indicators.

f) Using statistical analysis methods, such as linear regression models, on trade data concerning individual, non-aggregated imports and exports.

g) Comparing export information with tax declarations to detect discrepancies.

h) Paying particular attention to trade transactions that display known red flag indicators of TBML/FT activity.

i) Cross-comparing known typologies of risk (such as those identified in the FATF Typologies Report on Trade-based Money Laundering[4]) with trade data, information on cross-border monetary transfers associated with the payment of goods, intelligence, tax and wealth information.

j) Taking appropriate follow-up action when anomalies and discrepancies in trade and financial transactions are identified. Depending on the circumstances, appropriate follow-up action could involve asking the trader for further explanation and supporting documents; auditing traders who have presented discrepancies to check the volume of their business, regularity of their operations,

[4] FATF Typologies Report on Trade-based Money Laundering dated 23 June 2006.

the kind of goods exported, and connections with organised crime or any other illicit activity; and/or making the completed analysis available to the investigative authorities.

14. Providing services to their customers who are engaging in trade transactions, financial institutions also play an important role in the detection of TBML/FT. Consequently, it is best practice to include in training programmes for banking supervisors a focus on the importance of evaluating the adequacy of a bank's policies, procedures and processes for handling trade finance activities. Specific aspects to cover include:

a) Assessing the adequacy of a bank's systems for managing the risks associated with trade finance activities, including whether the bank effectively identifies and monitors its trade finance portfolio for suspicious or unusual activities, particularly those that pose a higher risk for money laundering.

b) Determining whether a bank's system for monitoring trade finance activities for suspicious activities, and for reporting suspicious activities, is adequate, given the bank's size, complexity, location, and types of customer relationships.

c) Sample testing trade finance accounts with a view to verifying whether the bank is meeting its customer due diligence, record keeping, monitoring and reporting obligations.

d) Providing AML training to financial institutions' global trade services departments and personnel.[5]

15. Countries are also encouraged to conduct outreach and awareness raising to the private sector concerning TBML/FT issues. The issues covered by such outreach could include an explanation of how trade finance activities may be vulnerable to abuse by terrorist and other criminals, a description of the national measures which have been implemented to counter such activity, information concerning TBML/FT typologies (*i.e.* methods, trends and techniques), red flag indicators and sanitised case studies. Financial institutions could be required to cover these same issues in their internal training programs, policies and controls. Feedback from the private sector on their experience in handling trade finance and implementing measures to combat TBML/FT could also be incorporated into training programmes, as appropriate.

16. To ensure that a sufficiently wide audience benefits from awareness raising and training on TBML/FT, countries are encouraged to consider using a combination of delivery methods, such as: offering or participating in conferences, seminars, workshops and other events, including those organised by the private sector; making presentations; holding inter-agency meetings; developing internet-based learning tools (e-learning); publishing guidance; posting information on the websites of competent authorities; including relevant information in the annual reports or other publications of competent authorities; or sending relevant materials to contacts directly. In the case of financial institutions, such materials could be sent to individual institutions directly or through their supervisor.

Typologies and red flag indicators

17. Another basic principle guiding the establishment of these best practices is that countries could agree to make case studies and red flag indicators identified in the typologies report[6] available to competent authorities and financial institutions.

[5] . Currently, many financial institutions focus their AML training at the customer level and not at their personnel working in their trade services departments.

18. Consistent with this basic principle, countries are encouraged to disseminate TBML/FT typologies, red flag indicators and sanitised case studies (particularly those identified in the FATF Typologies Report on Trade-based Money Laundering) to financial institutions and all competent authorities which the country has identified as being relevant to the fight against TBML/FT. Training programmes for both competent authorities and financial institutions could also include such information. Additionally, financial institutions could be encouraged to include these materials in their internal guidance and training manuals, and to keep their employees informed of developments in the area of TBML/FT.

19. Since TBML/FT has received relatively little attention from policy makers to date, it is important to continue increasing the pool of knowledge in this area. Consequently, countries are encouraged to conduct further study of TBML/FT at the national and regional level. Mechanisms for further study include: periodic joint meetings of relevant domestic authorities (*e.g.* trade and investigative authorities, customs agencies and the FIU) to discuss and share new and emerging TBML/FT trends and patterns; joint investigations or collaboration with foreign authorities; and knowledge sharing through the co-ordination of and participation in the work of relevant international and regional organisations such as the FATF, FATF-style Regional Bodies, Egmont Group, Interpol, Europol, World Trade Organisation (WTO) and the World Customs Organisation (WCO). Consultation with the private sector is also encouraged. For instance, some financial institutions may be able to contribute trade-specific red flag indicators which have been developed in-house for their own trade finance specialists.

Domestic mechanisms to link the work of relevant authorities

20. A review of the current practices of various jurisdictions shows that most countries would benefit from more effective information sharing among competent authorities at the domestic level, which leads to the following basic principle. In order to ensure that the expertise of competent authorities includes a focus on combating TBML/FT, jurisdictions could develop a domestic mechanism to link the work of authorities responsible for collecting, analysing and storing trade data with authorities responsible for investigating money laundering and terrorist financing.

21. In keeping with this basic principle, it is best practice for countries to first identify where trade data and relevant financial information are being stored. For instance, the responsibility of collecting and storing trade data may be shared by more than one agency (*e.g.* a customs agency, a department of statistics, a trade ministry, et cetera). Likewise, relevant financial information, including information relating to trade finance, may be held by trade authorities, the FIU, and/or the tax authorities. The next step is to ensure that there are clear and effective gateways, mechanisms or channels that allow the investigative authorities access, directly or indirectly, on a timely basis to trade data and relevant financial information, consistent with domestic privacy and data protection laws.

22. The following are examples of gateways, mechanisms or channels that can be used to facilitate information sharing among trade and investigative authorities that can be used in accordance with the national legal framework: memoranda of understanding, information sharing agreements, the use of liaison officers and the establishment of multi-agency task forces. Another possibility is to establish a specialised unit that is designated responsibility for monitoring imports and exports, analysing trade data and identifying anomalies with a view to detecting TBML/FT and other illicit activity, and supporting related investigations and prosecutions. The Trade Transparency Unit (TTU) concept, as established by some countries, is one such model.[7] It is best practice in this area to identify and address practical obstacles to

[6] . FATF Typologies Report on Trade-based Money Laundering dated 23 June 2006.

[7] TTU staff have experience in conducting financial, money laundering and trade fraud investigations, and also have access to a wide range of information, including customs information on cargo movements, trade data and financial information collected by the FIU. The location of a TTU would be dependent on where it

information sharing. For instance, where relevant information is held by authorities that are not yet an integral part of the traditional AML/CFT framework, information sharing gateways, mechanisms or channels may need to be established, preferably in conjunction with awareness raising and training in TBML/FT issues. Technical impediments, such as incompatible computer systems, could be addressed through the development of a single consolidated software platform for sharing information among trade and investigative authorities. Legal barriers might be addressed by having the competent authorities enter into a memorandum of understanding which covers information exchange. A lack of capacity to respond to information requests concerning TBML/FT could be managed by allocating additional resources or providing more training. In all cases, however, information exchange could only be conducted in an authorised manner and consistent with a country's domestic privacy and data protection laws.

23. Countries are encouraged to ensure that the FIU is notified about detections of possible TBML/FT, either through a system whereby the FIU is notified about suspicious trade transactions or by making the information available to the FIU in some other way. In such cases, the FIU could be authorised to obtain from other competent authorities (including the trade authorities, customs agency and investigative authorities) and reporting entities (*e.g.* financial institutions) where appropriate, additional information needed to properly undertake its functions. The systematic receipt of electronic funds transfers by FIUs may have value in assisting in the identification of TBML/FT.

Data protection and privacy

24. It is a basic principle that the collection and exchange of trade data shall only be conducted in an authorised manner and consistent with a country's domestic privacy and data protection laws.

25. Consistent with this basic principle, countries are encouraged to clearly specify the circumstances under which trade data may be disseminated and the legal basis for doing so. This includes clearly elaborating any available exemptions to domestic privacy and data protection laws. For instance, in some cases, trade data may be released if certain conditions are placed on the use of the information (*e.g.* the information will be used only for the purpose of fulfilling the receiving agency's functions, or for the purpose of investigating money laundering or terrorist financing) or if the receiving agency gives an undertaking not to use the information or further disclose it except for authorised purposes.

26. Where domestic privacy and data protection laws inhibit the dissemination of data at the domestic level, countries are encouraged to assess the underlying reasons for a specific protection provisions, and balance it against the potential benefits from future use of the data. For instance, pilot programmes could be undertaken to study the possible effects of such dissemination (*e.g.* by concluding limited memoranda of understanding between competent authorities).

27. It is best practice in this area to collect and maintain trade data and other relevant information in a national electronic secure database which can only be accessed by the appropriate authorities for the purpose of discharging their official duties. Ideally, specialised analytical and data mining software could be available to facilitate the analysis of trade data. Countries are also encouraged to use software rules that are designed to redact sensitive or identifying information from trade data, so that it can be used for trend analysis or information exchanges with other authorities. Sanitising trade data in this way has proven to be an effective way of sharing trade data with foreign authorities, without violating domestic privacy and data protection laws.[8]

would have the most value and be most efficient. Not unlike an FIU, different countries could house their respective TTU in different government departments.

[8] This practice is in use by TTUs to comply with partnering nations' domestic and privacy protection laws.

International co-operation

28. Another basic principle that guides the establishment of these best practices is that, in order to facilitate international co-operation in combating TBML/FT, countries could establish clear and effective gateways, subject to appropriate controls and safeguards and existing legal frameworks, to facilitate the prompt and effective exchange of trade data and other relevant information, on a case-by-case basis or as otherwise appropriate, among authorised counterparts.

29. In line with this basic principle, countries are encouraged to provide the widest possible range of mutual legal assistance in TBML/FT investigations and prosecutions. This includes being able to share trade data and relevant financial information with other countries through the framework of mutual legal assistance in a timely, constructive and effective manner. Countries could also be able to co-operate in joint TBML/FT investigations.

30. It is best practice in this area for countries to be able to share trade data directly with their foreign counterparts (*i.e.* administrative assistance). Clear and effective gateways, mechanisms or channels that will facilitate such information exchange could be established. For example, the TTUs of some countries share a single database which allows them to manage and match trade data. This mechanism is further enhanced by having foreign liaison officers working within the TTU. Another, more common mechanism is a memorandum of understanding. Regional or international information exchange platforms may also be used to facilitate the exchange of trade data (*e.g.* the Customs Information System in the European Union or the Egmont Group Secure Network of FIUs). Where the sharing of specific trade information with foreign counterparts is prohibited, countries are encouraged to share sanitised trade data. Countries may also wish to explore other data exchange models based on different levels of statistical aggregation.

Legitimate trading activities

31. It is a basic principle that the above measures could be implemented with a view to ensuring that legitimate trading activities are not unreasonably hindered or obstructed.

32. Consistent with this basic principle, countries are encouraged to keep the following considerations in mind when implementing measures to combat TBML/FT: competitive neutrality, competition and economic efficiencies, the desirability of ensuring that regulatory considerations are addressed in a way that does not impose unnecessary financial and administrative burdens on reporting entities, and the risk that commercially sensitive information could be misused (*i.e.* for purposes other than combating TBML/FT).

33. A review of the current practices of various jurisdictions shows that the following measures can be implemented without hindering legitimate trading activities:

(a) Applying an intelligence, risk-based and target-based approach which makes consistent use of TBML/FT red flag indicators.

(b) Using data capture mechanisms such as Electronic Data Interchange (EDI), which is a set of standards for standardising the structure of information to be electronically exchanged between authorities, from one computer system to another, without human intervention and subject to appropriate data protection safeguards.

(c) Authorising traders that meet certain criteria to benefit from facilitations for customs controls or simplifications for customs rules (*e.g.* Member states of the European Union recognise Authorised Economic Operator (AEO) status which is granted to traders that meet the following criteria: an appropriate record of customs compliance, satisfactory management systems that allow appropriate customs controls, adequate security and safety standards, and proven solvency).

(d) Utilising the trade data that is gathered automatically from customs declaration forms thereby avoiding any extra burden for the traders who are involved in legitimate trade.

(e) Conducting non-intrusive inspections of goods being imported and exported using scanners.

(f) Having authorising domestic authorities (*e.g.* customs, FIU) share information either upon specific request or spontaneously.

(g) Providing information to foreign authorities and placing conditions on the use of such information.

(h) Establishing a Trade Transparency Unit to facilitate the sharing and analysis of import/export data. Because the system does not rely on real-time trade information to target data (the system uses historic data to identify anomalies that are indicative of TBML/FT), legitimate trading activities are not unreasonably hindered.