Financial Action Task Force

FATF/RTMG(2020)18/REV3

For Official Use **English - Or. English**

16 October 2020

Risk, Trends and Methods Group

TRADE-BASED MONEY LAUNDERING 2020 UPDATE: TRENDS AND DEVELOPMENTS

14 – 15 October 2020, Virtual Meeting

Issue: this document contains the revised Trade-Based Money Laundering 2020 Update: Trends and Developments report and communication and follow-up plan. This version incorporates changes agreed at the virtual RTMG meeting on 14 and 15 October 2020.

Action: For adoption

FATF-XXXII
This document is for official use by FATF members and observers only. It must not be made publicly available or distributed to third parties without prior authorisation from the FATF.

John CARLSON, Tel.: +(33-1) 45 24 79 46, John.CARLSON@fatf-gafi.org
Ivan UVAROV, Tel : +(33-1) 85 55 45 47, Ivan.UVAROV@fatf-gafi.org

JT03467004

Trade-Based Money Laundering 2020 Update: Trends and Developments

Paper for adoption

Issue:	This document contains the revised Trade-Based Money Laundering 2020 Update: Trends and Developments report and communication and follow-up plan. This version incorporates changes agreed at the virtual RTMG meeting on 14 and 15 October 2020.
Action:	For adoption.
Recommendation(s):	To adopt the attached report and communication and follow-up plan.
Timing:	Should the Plenary adopt the report, the Egmont Group will circulate it to its members for adoption through written procedure.

Background

1. In June 2020, RTMG discussed the progress made on the joint FATF/Egmont project on trade-based money laundering (TBML). In August and September 2020, delegations were invited to provide comments to the draft report. The report has also benefitted from the comments provided by selected private sector experts.

2. The attached version of the report (Annex A) incorporates feedback provided by project team members over August and September, comments from other delegations and selected private sector experts, and the outcomes of the RTMG virtual meeting held on 14 and 15 October 2020.

Communication and follow-up plan

Objectives and target audience

3. As identified in the report, one of the most important challenges to the effective identification and disruption of TBML is a lack of understanding. This challenge has persisted since the adoption of the first FATF study on TBML in 2006. Insufficient knowledge about TBML impedes the ability of reporting entities to detect potential instances of TBML, while private sector companies involved in the trade chain may be inadvertently facilitating TBML. In turn, competent authorities may miss opportunities to detect and investigate TBML due to a low understanding of the phenomenon. Raising awareness about TBML among public and private sector experts is the key objective of this project.

4. The report also aims to provide guidance to public authorities on how to overcome this and other challenges to effective tackling of TBML. This includes recommendations on improving information sharing between competent authorities, use of national risk assessment processes to strengthen TBML understanding and communication with the private sector through public-private partnerships.

5. These two objectives determine the target audience of the report, which includes competent authorities responsible for detecting and investigating predicate offences and

ML/TF, experts from FIs and DNFBPs, as well as private sector companies involved in trade.

Communication and follow-up

6. Based on the above objectives and target audience, the co-leads propose the following steps to facilitate communication of the report:

- **Publication of the report.** Publication of the report on the FATF web site will allow experts from both the public and private sector to easily access the document.
- **Developing targeted handouts**. Developing targeted handouts reflecting the report's findings in a visually attractive manner should facilitate communication to competent authorities and relevant private sector entities. Such handouts may cover TBML techniques and risks, difference between TBML and other trade-related crimes, and key recommendations identified in the report.
- **Translation of the report.** Delegations are encouraged to translate the report into other languages to enable communication of the report's findings to a broader audience. The Secretariat will invite delegations and FSRB Secretariats to provide translated versions of the report for posting on the FATF website alongside the original document.
- **Creating videos about TBML.** As identified above, the report aims to raise awareness about TBML amongst a broad audience. At the same time, promoting FATF products outside delegations and the expert community has always been challenging. Developing videos about various TBML risks and techniques should contribute allow for a broader outreach. Subject to the available resource, such videos may involve the project co-leads presenting the report's findings in a simple manner, infographics and other visual material.
- **Organising a webinar.** Subject to the resource available to the Secretariat and delegations, organising a webinar about TBML should also increase awareness across the expert community. This may include a detailed discussion of the key aspects of TBML and the steps that jurisdictions may take to improve the effectiveness of their AML/CFT systems to tackle TBML.

7. As noted above, the report identified several steps that jurisdictions may take to improve measures against TBML, including facilitating domestic information sharing and enhancing collaboration with the private sector through PPPs. However, it may take substantial time for jurisdictions to apply any of these measures so they lead to a notable effect on the ground. Having this feedback may give other delegations a valuable insight into practical implementation of the report's findings. Therefore, **should delegations agree to this proposal, they will be invited to report on the use of the report in a 1-1.5 year timeframe**. This objective can be achieved by circulating a short survey to delegations in the set timeframe.

Recommendations and next steps

8. To adopt the attached report and communication and follow-up plan.

9. Should the Plenary adopt the report, the Egmont Group will circulate it to its members for adoption through written procedure.

10. At its meeting on 14 and 15 October 2020, RTMG also discussed the list of TBML risk indicators annexed to the draft report [Annex B, FATF/RTMG(2020)18/REV2] and agreed to continue work to refine the list in order to develop a public list of TBML risk indicators. Subject to Plenary's approval, this work should be accomplished during the next inter plenary cycle, i.e. before the February 2021 plenary meeting, with the intention to agree the final list for adoption through written procedure.

Annex A. TRADE-BASED MONEY LAUNDERING 2020 UPDATE: TRENDS AND DEVELOPMENTS

Table of contents

List of Acronyms

AML/CFT	Anti-money laundering/Countering the financing of terrorism
APG	Asia Pacific Group on Money Laundering
BMPE	Black Market Peso Exchange
BO	Beneficial owner
DNFBP	Designated non-financial businesses and professions
LEA	Law Enforcement Authorities
ML	Money laundering
MVTS	Money value transfer service
FATF	Financial Action Task Force
FI	Financial institution
FIU	Financial intelligence unit
FSRB	FATF-style regional body
NRA	National risk assessment
PPP	Public-private partnership
PML	Professional money launderers
OCG	Organised criminal groups
SBML	Services-based money laundering
TBML	Trade-based money laundering
TBTF	Trade-based terrorist financing
TBML/TF	Trade-based money laundering and terrorist financing
TF	Terrorist financing

1. Executive Summary

1. This report is a companion piece to earlier Financial Action Taskforce (FATF) and FATF-style Regional Body (FSRB) documents focusing on trade-based money laundering (TBML), such as the 2006 landmark study, the 2008 best practices paper, and the 2012 report by the Asia Pacific Group on Money Laundering (APG).

2. This report complements the insight generated by those original publications, while benefiting from additional input from the Egmont Group of Financial Intelligence Units (Egmont Group), national and international private sector institutions, and multi-lateral bodies. Capturing this public and private sector insight has created a comprehensive study outlining the extent to which TBML remains a significant money laundering (ML) risk, while noting the consolidation of already established TBML techniques, and newer developments in respect of illicit cash integration[1]. It also covers the risk of trade-based terrorist financing (TBTF), to build awareness and understanding of how terrorist financiers can exploit trade processes.

3. It also reflects on progress made since the APG's report, including promotion of its key findings about practical enhancements to risk analysis, assessment and mitigation. While the report recognises there are still significant challenges in achieving successful criminal prosecutions of TBML, it notes the development of additional initiatives, tools and capabilities that are improving efforts to detect and disrupt TBML schemes. This includes advanced IT and risk-assessment systems, and deeper and more systematic cooperation between the public and private sectors.

4. The report is intended for an extensive audience, including competent authorities tasked with identifying, investigating, or prosecuting TBML/TF; financial institutions (FIs); designated non-financial businesses and professions (DNFBPs) that may be at risk from TBML/TF exploitation or identify aspects of it, without realising what it means; and other interlocutors involved in regional or global supply chains, such as freight forwarders and customs brokers that hold relevant and meaningful trade or financing data.

1.1. Key findings

5. Trade can be inherently complex and complicated, reflecting the nature of interconnected supply chains stretching around the world. These are exploited by Organised Criminal Groups (OCGs), Professional Money Launderers (PMLs), and Terrorist Financing (TF) networks, to facilitate myriad types of financial flows, including the laundering of proceeds of crime, such as from drug trafficking; the financing of terrorism; and the evasion of sanctions.

6. Report contributors noted the continued exploitation of TBML techniques[2] first identified in the 2006 FATF study. The continue to be used for ML purposes as they are highly flexible and adaptable, despite changes in global trading patterns and the growth of new markets. These techniques are particularly effective when there is a complicit relationship between the importer and exporter, who are actively misrepresenting an aspect of the trade or the associated invoice settlement process. Therefore, authorities can have a

[1] In very simple terms, trade involves the transfer of goods or services from one person or entity to another. The terms of trade, such as the volume and value of the good or service, methods of transportation, how invoices will be settled, by whom and by when, can vary from one entity to another. These are very basic examples of adding complexity.
[2] These techniques were described in the initial 2006 FATF report and include: under- or over-invoicing of goods; under- or over-valuation of goods, and/or phantom shipments, where no goods move at all.

greater impact if they can disrupt these complicit actors, whether through criminal prosecution or another form of disruption – e.g. removing their authority to trade.

7. **In addition, exploitation of trade financing processes was a common theme noted by private sector contributors. The APG's report promoted the importance of public sector bodies deepening their understanding of these processes, to complement their existing knowledge of predicate offences linked to TBML. This remains a key finding for this report, as greater awareness about all aspects of the trade process, including how different financing processes are managed, would likely increase opportunities to detect and successfully disrupt TBML/TF.**

8. The report takes stock of current TBML risks, including the exploitation of new or existing methods of introducing illicit cash into the financial system. Despite the growth in technology-enabled payment methods, case studies highlight the reliance on Black Market Peso Exchange (BMPE). In addition, other forms of illicit cash integration were noted, such as the exploitation of surrogate shopping[3] or the infiltration of legitimate supply chains[4].

9. While there can be significant intersection between TBML or TBTF schemes and exploitation of shell or front companies, they do not feature in all TBML/TF schemes. When they are used, they can support the integration of funds, while providing an additional benefit of hiding the beneficial owners.

10. The report notes the continued occurrence of third-party intermediaries, often as part of the financial settlement process. These third-party intermediaries, linked to the OCG, PML or terrorist financier, can quickly integrate into the transaction chain, creating additional distance between their activities and the TBML or TBTF scheme.

11. **While financial institutions were aware of the risks associated with third-party intermediaries, the report acknowledges that others in the supply chain, such as legitimate importers or exporters, or those with an oversight role, such as auditors or accountants, may not question why an entirely unrelated third-party is involved in the payment settlement process.**

12. All contributors noted there are still challenges in routinely identifying and combating TBML/TF. Issues flagged in the 2006 study and expanded in the 2012 report, remain. For example, challenges in ensuring systematic and consistent cooperation, both domestically and internationally, can hamper detection and disruption of TBML and TBTF schemes.

13. **Relevant trade data is held across multiple stakeholders with restrictions about the extent to which this data is shared, both operationally and in bulk. Newer challenges highlighted include the growth in online businesses, restricting scope for proactive compliance activity, and new technologies and the digitalisation of trade processes, increasing the speed of trade operations.**

14. At the same time, the report reflects on several new initiatives and continued maturity of others, which aim to address these challenges, and increase capability across the trade system to identify and respond to TBML and TBTF. For example, numerous countries

[3] Surrogate shoppers can act on behalf of wealthy individuals, who might face restrictions in purchasing higher-value goods because of stringent currency controls. One such example of this is known as Daigou (which literally means surrogate shopping) whereby individuals or syndicated groups of exporters outside Asian countries purchase mainly luxury goods for customers in those countries.

[4] This infiltration may not necessarily result in the subsequent growth of 'common TBML techniques. In some instances, nothing about the trading relationship changes, other than an increase in illicit cash integrated into the importing company. This and the exploitation of surrogate shopping are explored in more detail in the TBML risk and trends section of the report.

have established Public Private Partnership (PPP) initiatives, where public and private sector stakeholders cooperate to share knowledge and expertise on critical financial crime risks, including TBML. This approach to collaboration with the private sector has also been adopted by some international bodies.

15. There has also been a growth in comprehensive studies on trade-related activities[5], and competent authorities are engaging in new forms of bi-lateral and multi-lateral intelligence sharing and investigation initiatives[6] that are disrupting TBML/TF. The report reflects on these initiatives and other examples of tackling TBML/TF best practice.

16. **At the strategic level, FATF's introduction of a risk-based approach[7] to AML/CFT in 2012, is arguably the most fundamental revision to the FATF Standards in recent years. It encourages jurisdictions to undertake systematic analysis of their exposure to ML/TF risks, including TBML. A primary output of this analysis is often a National Risk Assessment (NRA), which can act as a bridge between the public and private sector's understanding of threats and vulnerabilities. It can help ensure there is consistency of risk understanding, and inform the development of risk-based policies, procedures and/or legislation.**

17. The report provides several examples of NRAs that have identified exposure to TBML and is complemented by case studies of how private sector institutions have adapted their risk-assessment processes to better detect TBML. Given the international nature of the risk, this process was recognised as vital in encouraging jurisdictions and institutions to consider their exposure to TBML/TF, particularly those coming to the risk from a new perspective, whether that is because of a growth in trade activity, an increase in company formation processes or expansion of their financial services market.

1.2. Conclusion

18. The report aims to present complex issues in an accessible, easy-to-understand way. It has relevance to countries with already well-developed systems and processes to identify and disrupt TBML or TBTF, and to those starting on that journey because they have noted a growth in suspicious activity linked to trade transactions. It provides a toolkit of ideas and initiatives that have delivered impact in combatting TBML and TBTF schemes and these can be adapted by jurisdictions to suit their domestic circumstances. For example, if there are restrictions on the extent to which public and private sectors can share actionable ML or TF intelligence, any PPP can focus more on establishing a meaningful dialogue on strategic threat and risk understanding.

19. The overarching theme of the report is one of vigilance, with competent authorities, private sector institutions, and other participants in global supply chains encouraged to use the report as a guide.

[5] For example, the Wolfsberg Group, the International Chamber of Commerce and the Bankers Association for Finance and Trade (BAFT) have independently and cooperatively produced several insightful guides on aspects of trade-based money laundering such as the 2019 Trade Finance Principles paper and appendices.

[6] For example, in 2018 the United States, Canada, the Netherlands, Australia and the United Kingdom's respective tax authorities established the Joint Chiefs of Global Tax Investigation (the J5), to investigate those who enable transnational tax crimes and money laundering. Tax evasion is a recognised predicate offence linked to TBML.

[7] The FATF website includes several helpful resources to explain the revisions, but a risk based approach means jurisdictions, competent authorities and regulated entities assess and understand the ML and TF risks to which they are exposed, and take appropriate mitigation measures in accordance with the level of risk.

2. Introduction

2.1. Background

20. FATF's 2006 study of TBML provided a comprehensive and detailed assessment of the phenomenon, identifying the types of trade activity exploited in TBML schemes. The report recognised TBML as one of the three main methods by which OCGs move funds and assets for the purpose of disguising its origin. This was quickly followed by a TBML Best Practices paper in 2008 to assist authorities with addressing the risks identified.

21. The APG produced an updated report in 2012, building on the original study, while noting several issues that hampered the effective identification of TBML and its subsequent investigation. In addition to these specific reports, TBML has also featured in several other FATF documents, including its prevalence as it relates to the exploitation of Free Trade Zones (2010) and its use by Professional Money Laundering Networks (2018).

22. Given the dynamic nature of international trade, including the diversity of tradable goods and services, the involvement of multiple parties, and the speed of trade transactions, TBML remains a profound and significant risk. For context, the WTO Statistical Review of 2019[8] notes the volume of the global trade in world merchandise (i.e. goods) trade grew by 3% in 2018, while the value of that trade increased by 10% to $19.67 trillion, driven, in part, by a significant growth of fuels and mining products, at 23%. This growth may resonate with several respondents noting the exploitation of fuels and mining products in TBML schemes. The report also noted that world exports of merchandise trade increased 20% in value over this period.

23. The same report also noted that developing economies outperformed or equalled the performance of developed economies in world trade, in most of the past ten years. This would suggest expansion into previously underexploited markets, both in terms of goods and services, which have created new opportunities for the manipulation of trade activity by OCGs, PMLs and terrorist financiers.

24. This report is a companion document to those earlier assessments but draws on additional insight and expertise from across the FATF Global Network, the Egmont Group of Financial Intelligence Units, private sector institutions, and other multi-lateral bodies. It represents a comprehensive, fresh look at TBML methodologies and mitigating measures, including the impact of new initiatives such as the establishment of public-private partnerships (PPPs). It also provides fresh insight into TBTF to build awareness and understanding of how terrorist financiers can and do exploit trade processes.

2.2. Purpose and report structure

25. The report is intended for an extensive audience, including competent authorities tasked with identifying, investigating, and prosecuting ML or TF, FIs and DNFBPs that may be at risk from TBML/TF exploitation or identify aspects of it, without realising what it means, and other stakeholders involved in global supply chains that may find themselves exposed to TBML/TF schemes.

26. It aims to describe the complexities of international trade, and associated financing mechanisms, in an easy-to-understand way, providing clarity for key stakeholders involved in mitigating TBML/TF risks. However, given the complexities of the subject, the report also highlights insightful and informative works by others that may be useful in further developing understanding of TBML/TF.

[8] World Trade Statistical Review in 2019: https://www.wto.org/english/res_e/statis_e/wts2019_e/wts2019chapter02_e.pdf

27. The collaboration with the Egmont Group was a significant opportunity to capture input from FIUs on sources and techniques for detecting TBML, in addition to enriching the identification of TBML/TF schemes and associated risk indicators. This complements input from law enforcement agencies operating at the vanguard of detecting, investigating, and prosecuting TBML/TF networks, and experience from custom services, with multiple case studies provided to support further successful interventions.

28. The third significant contribution comes from several national and international FIs, which provides additional insight of the risk, while highlighting examples of successful TBML scheme disruptions that are alternative measures to criminal investigations and prosecutions.

29. Taking the above into account, the report is structured to achieve the following objectives:

Section 3: Definitions and trade financing activities

This section:

- Consolidates previous definitions of TBML and offers clarification on TBTF, which readers can use to improve their understanding of TBML/TF. This is particularly pertinent for those who are new to the phenomenon or may not have a defined role in assessing their exposure to the risk[9]. This toolkit also clarifies the differences between TBML and trade-related predicate offences, such as smuggling.
- Outlines, in basic terms, trade process and financing to assist public sector bodies in deepening their understanding of how these are exploited in TBML/TF schemes. The need for this was a key recommendation in the 2012 report and was reflected as an existing gap by report contributors.

Section 4: TBML Risks and Trends

This section:

- Identifies how members of the FATF Global Network have increased their awareness, assessment, and identification of TBML/TF. This will highlight examples of risk analysis and assessment from across the public and private sector. These examples are intended to provide a steer for jurisdictions, competent authorities and/or other private sector institutions to support their shared understanding of TBML/TF risk.
- Provides a summary of economic sectors and products at risk of TBML/TF. These are by no means an exhaustive list but are provided to assist competent authorities with less mature TBML/TF detection processes a starting point for future analysis of risk and threat.
- Assess the extent to which TBML is still characterised by what the 2006 report described as 'basic' TBML techniques but are more accurately considered 'common' techniques. These are broadly categorised as involving misrepresentation of goods and/or value. It also reflects on the continued use of Black Market Peso Exchange (BMPE).
- Summarises key TBML/TF risks, reflecting on newer methods of cash integration such as the exploitation of surrogate shopper networks, and the infiltration of

[9] This would cover firms not required to undertake AML/CFT activities, but that are involved in trade transactions and may be at risk of TBML/TF facilitation. For example, freight forwarders or customs brokers.

legitimate supply chains that do not rely on misrepresentation of any aspect of the trade process.

- Shares insight about TBTF, recognising the additional complexities in its detection compared with TBML. It also notes lessons jurisdictions, competent authorities or private sector institutions can learn from those who have identified and successfully tackled TBTF.

Section 5: Challenges to countering TBML

This section:

- Reviews current operational challenges that hamper the successful identification, classification, investigation, or prosecution of TBML or TBTF schemes. These are mapped against similar analysis completed in the 2012 assessment, with previous key findings reiterated to encourage further positive action across the FATF Global Network.

Section 6: Measures and best practices to counter TBML

This section:

- Reflects on the introduction of new initiatives aimed at improving cooperation within and across jurisdictions, including the establishment of PPPs and other forms of multi-agency taskforces.
- Provides new and innovative approaches to risk identification using IT and enhanced system-wide analysis. Lessons learned are distilled from these activities that may assist in a more integrated disruption and investigation response.

30. As such, it is anticipated the report provokes consideration, debate, and further cross-community engagement about the risk, given the inherent flexibility of TBML/TF methods and sectors or commodities exploited.

2.3. Methodology

31. The report has benefited from the support and direction of a project team made up of members from across the FATF Global Network and the Egmont Group. To generate the insights and findings for the report, the project team – in addition to convening project team meetings – used the following processes:

- The preparation and distribution of questionnaires. The first questionnaire sought contributions from competent authorities across the FATF Global Network to generate their insight on TBML, including the identification of sectors exploited, challenges in advancing investigations and/or securing prosecutions, and case studies of successful TBML disruptions. The second questionnaire was targeted at the private sector to elicit its thoughts on TBML, including any activities they have developed that have improved their understanding and/or identification of the risk. The third questionnaire was developed by the Egmont Group's Information Exchange Working Group (IEWG) to gather case studies, experiences, challenges, best practices, and useful risk indicators from participating FIUs.
- The reiteration of key learning points and findings from previous FATF reports about TBML, primarily the APG's 2012 report. This includes updates to how the 'processes of trade finance' were explained in the 2012 report, reflecting the growth and adaptation of global trade.

- The review and refinement of previous 'red flag' indicators, considering additional insight generated by the questionnaires and engagement with a range of public and private sector firms.
- A limited literature review of open source documentation that promotes best practice in tackling TBML. This includes the World Customs Organisation (WCO) and the Egmont Group's Customs-FIU Cooperation Handbook, and a 2019 Trade Finance Principles paper co-authored by the Wolfsberg Group, the International Chamber of Commerce (ICC), and the Bankers Association of Finance and Trade (BAFT)[10].

32. Each section of the report reflects feedback from the questionnaires, with case studies provided to highlight elements of TBML/TF schemes worthy of note. In developing the section about risks and trends, the report identifies several sectors and commodities currently seen by questionnaire respondents, both in the public and private sectors, in their TBML investigations. However, as one questionnaire respondent noted, **OCGs, PMLs and terrorist financiers will exploit any sector, commodity, or service where they perceive an opportunity.**

33. The overarching theme of the report is one of vigilance, with competent authorities, private sector institutions, and other participants in global supply chains encouraged to use the report as a guide.

[10] https://www.wolfsberg-principles.com/sites/default/files/wb/Trade%20Finance%20Principles%202019.pdf

3. Definitions and trade financing processes

3.1. Defining TBML and TBTF

34. Trade exploitation presents opportunities for OCGs, PMLs and terrorist financiers to frustrate identification and intervention by authorities and financial institutions. It can also support a broad range of other illicit financial flows, including capital flight, sanctions evasion, customs violations, and tax evasion. To help simplify the issues, this section of the report:

- Reaffirms the previous FATF definition of TBML and suggests a practical definition of TBTF;
- Describes why TBML differs from trade-related predicate offences by focusing on intent;
- Describes the basics of those trade financing techniques exploited in TBML/TF schemes;

3.1.1. TBML versus trade-related predicate offences

35. TBML, as defined in the 2006 FATF report, is "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origin or finance their activities".

36. In summary, the primary aim of any TBML scheme is the **deliberate** movement of illicit proceeds through the exploitation of trade transactions. In doing so, criminals may engage in a range of other potentially unlawful activities, such as preparing false invoices, mischaracterizing goods to circumvent controls, and other customs and tax violations. **But the aim of TBML – unlike trade-related predicate offences – is not the movement of goods, but rather the movement of money, which the trade transactions facilitate**.

37. Another key distinction of TBML schemes is the involvement of PMLs. Whereas criminals perpetrating trade-related predicate offences are usually the ultimate beneficiaries of those illicit proceeds, PMLs offer specialist expertise using a range of ML techniques (e.g. TBML) to diversify their risk exposure. These PMLs take receipt of the criminal proceeds on behalf of the OCG and transfer or convert those proceeds, including via TBML schemes, before passing them back to the OCG, minus the payment of their fee or commission.

3.1.2. Defining trade-based terrorist financing

38. TBTF uses the same trade processes as TBML but has a significant and fundamental difference – proceeds or value moved can come from both legitimate and illegitimate sources, increasing the complexity in detecting and disrupting TBTF.

39. **As such, the report defines TBTF as "disguising the movement of value through the use of trade transactions in an attempt to finance terrorism, whether from legitimate or illegitimate sources".**

40. While the report notes the additional layers of complexity in detecting TBTF, the case studies referenced, and analysis of other material provided[11], identifies some aspects of TBTF that may help authorities to strengthen their understanding of TBTF schemes.

[11] For example, a sub-typology suggested is the procurement of items for use by terrorist groups. This includes typical goods such as firearms, but also logistical equipment and weaponizable technology such as used vehicles or drones to conflict zones.

3.2. Trade process and financing

41. This next section summarises the common types of trade financing identified in previous FATF reports. It is by no means an exhaustive list but is provided to ensure a basic level of understanding.

42. International trade involves a range of risks for the parties involved, which leads to uncertainty over the timing of payments between the exporter and importer. This creates tension along the supply chain, which can have negative consequences for both the importer and exporter.

43. Trade processes and financing have adapted to address this tension, while still supporting the growth of the global marketplace. As such, there are five primary methods of payment for international transactions, summarised in Table 3.1. These are ranked in terms of preference for the importer or exporter – so the least preferable method for the importer is usually cash in advance, as they must pay the exporter ahead of receiving the goods, but this is the most preferable method for the exporter.

Table 3.1. Payment processes and level of risk management

	Least Preferable	Less Preferable	Neutral	More Preferable	Most Preferable
Exporter	Consignment	Open Account	Documentary collections	Letters of Credit	Cash in advance
Importer	Cash in advance	Letters of Credit	Documentary collections	Open Account	Consignment

Source: Adapted from https://2016.export.gov/tradefinanceguide/eg_main_043221.asp/

44. Contributors noted open account and documentary collections as being the most prominent in their TBML analysis and investigation activities. In fact, the Wolfsberg Group notes approximately 80% of international trade processed by FIs is open account trading. However, it should be noted that just because other types of trade finance are not referenced, does not mean they aren't exploited in TBML schemes. Nevertheless, as a method for systematically disguising the proceeds of crime, an importer routinely paying cash in advance is likely to arouse the suspicion of authorities or FIs.

3.2.1. Open account

45. The United Nation's Trade Facilitation Implementation Guide notes that an "open account transaction is a sale where the goods are shipped and delivered before payment is due". Payment is usually made by a set time period, anywhere between 30 and 90 days after receipt of the good or service. This method is frequently found in TBML schemes because FIs have a reduced role, meaning less oversight than aspects of the documentary collection process. FIs can struggle to accurately or consistently asses the legitimacy of the customer's operations, whether through automated or manual transaction monitoring.

46. This issue was highlighted in the APG's report, which described it as "creating a disconnect between the movement of the underlying trade and the money used to finance it"[12]. This disconnect is then exploited by OCGs, PMLs or terrorist financiers, using specific loopholes or gaps, in a compartmentalised fashion, mitigating their risk exposure. Further

[12] The 2012 report includes a comprehensive analysis of a range of open account facilities, including factoring, both export and import, forfeiting, pre- and post-shipment finance, and credit arrangements between buyers and suppliers.

complexity can be added by using third-party intermediaries in multiple jurisdictions to frustrate law enforcement or FI detection and disruption.

47. However, it is important to stress that open account trading is a fundamental part of the global trading process, so the potentially easy answer of increasing regulation of open account trading is not logistically or economically viable. Later sections of this report highlight existing and newer initiatives that increase opportunities to spot ML or TF exploitation, with additional reference material available online setting out compliance procedures, for open account trading, to increase TBML detection.

3.2.2. Documentary collections

48. In documentary collection, the exporter requests payment by presenting shipping and collection documents for the traded goods to its FI. The FI then forwards these documents to the importer's FI, who then transfers the funds to the exporter's FI, who will subsequently credit those funds to the exporter.

49. However, despite a perceived increase in role for FIs, it is limited as they do not necessarily verify the documents. In addition, documents are not always standardised, increasing the risk of TBML exploitation through fictitious or false invoicing. However, when these documents can be checked and assured, certain data points can be used to spot TBML, including:

- Use of a personal email address in lieu of a legitimate business email.
- Subject to an FI's data storage capabilities, the obvious recycling of previous documentation with few or no edits, including something as basic as the date.
- The complete lack of any trading presence of the exporter, following research by the FI. This included the use of residential rather than business premises for exporters providing significant quantities of goods.

4. TBML Risks and Trends

50. The following section explores TBML risks and trends in more detail. In line with the report's objectives, this section:

- Acknowledges the requirements of the existing FATF Recommendations, to give jurisdictions confidence in using or enhancing their existing AML/CFT legal framework, policies, and procedures to increase their ability to identify and disrupt TBML/TF.
- Illustrates how jurisdictions and firms achieve an understanding of their exposure to TBML and TBTF and the process for developing that understanding, including via any NRA process, or risk-specific threat assessments, for example, the exploitation of a jurisdiction's corporate structures in facilitating TBML.
- Highlights the most common types of predicate offences involving TBML as a preferred or significant ML mechanism. The report does not focus on these predicate offences in detail but references them to encourage competent authorities to revisit historic or ongoing investigations into those predicate offences to determine if TBML is involved.
- Summarises the economic sectors or products vulnerable to TBML/TF exploitation. As with predicate offences, these are provided to guide competent authorities or regulated firms in any review of those sectors or products to determine if they are exploited for TBML/TF. It is by no means a definitive list but illustrates the broad range of sectors and products that OCGs, PMLs and terrorist financiers will exploit.
- Provides insight into the common TBML techniques that have been traditionally used by criminals, as well as outlining several newer TBML risks that have emerged.
- Notes the facets of services-based money laundering (SBML), albeit stressing that while it shares similarities with TBML, it is a totally different form of money laundering.

51. Notwithstanding this section's focus on risk, the report found that jurisdictions noted difficulties in attempting to indicatively quantify the value of their TBML/TF exposure. The main challenges include the complexity and growth of international trade, the challenges customs authorities faced in checking more than a fraction of international trade shipments[13], the cross-jurisdictional nature of TBML, and in some cases, limited understanding of FIs and their customers of TBML/TF exposure.

4.1. Risk-based approach to TBML

52. A significant change since the APG's 2012 report is the revisions to the FATF Recommendations and associated country evaluation procedures covering AML/CFT measures. This includes the development of an effectiveness assessment methodology, which is focused on the practical implementation of the AML/CFT measures, rather than just the transposition of the FATF Recommendations into domestic legislation. For example, the FATF Recommendations require a country to have in place a legal framework for the prosecution of ML offences, while the effectiveness assessment determines the extent to

[13] This activity can include a broad range of different data or documentary inputs, including but not restricted to – invoices, shipping documentation, associated customs documentation, physical spot checks. However, contributors noted that even having access to these inputs is no guarantee of detecting TBML, reflecting the need for cooperation with all trade chain participants.

which these offences, including TBML, are investigated and prosecuted in line with a country's risk profile.

53. This section is focused on the implementation of a risk based approach to ML/TF, which is a critical starting point for countries in assessing their risk exposure.

54. FATF Recommendation 1[14] requires countries to identify, assess, and understand their ML/TF risks, and implement subsequent preventative and mitigating measures, which are commensurate with the risks identified. This could include threats and vulnerabilities linked to TBML/TF. Countries often meet this requirement by developing NRA for ML and TF, some of which are publicly available in full or in a sanitised form. These are primarily driven by public sector bodies but can incorporate feedback from the private sector as part of the assessment development process.

55. While there are multiple ways of assessing ML/TF risk exposure to create the NRA, a country assesses several different inputs, including intelligence reports, suspicious transaction reports (STRs), threat assessments, investigation outcomes, and economic and social indicators, as well as the level of the threat and existing vulnerabilities[15].

56. The overarching theme from public sector contributors to this report was the association of TBML with a range of domestic and foreign predicate offences. This includes offences resulting in the smuggling of illicit or restricted commodities, such as drug trafficking, arms dealing or tobacco smuggling, with OCGs and PMLs re-exploiting the supply chain used to smuggle the goods to launder their criminal proceeds.

57. Others noted TBML schemes associated with predicate offences not reliant on commodity smuggling, such as tax evasion. These schemes, typically associated with PMLs, require the development of new supply chains and financial intermediaries as there was no pre-existing commodity supply chain to exploit. These TBML schemes were often multi-jurisdictional, not only exploiting trade sectors in the originating jurisdiction, but also impacting others through the exploitation of corporate services.

58. A handful of respondents referenced both actual and potential TBTF abuse and this insight is covered later in this section. However, most did not see abuse of the trade system in moving funds to facilitate terrorist acts, or on behalf of individual terrorists or groups.

59. While TBML or TBTF can occur in countries where trade is significant, contributors noted TBML/TF enabling activities – such as the misuse of corporate structures – can occur in a wide range of jurisdictions. OCGs, PMLs, and/or terrorist financiers exploit any potential loopholes or gaps, and the benefit of the NRA is challenging countries to think about risk exposure in terms of threat and vulnerability.

[14] Further details on specific FATF Recommendations are available on the FATF website – www.fatf-gafi.org

[15] See FATF's Guidance on National ML and TF Risk Assessment for further details of the process. http://www.fatf-gafi.org/publications/methodsandtrends/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

Box 4.1. German NRA and TBML

In December 2017, Germany launched its first NRA as part of its efforts to combat ML and TF. A total of 35 federal and local authorities were involved in the assessment, which was led by the Federal Ministry of Finance.

The first NRA highlighted the significance of TBML, because of Germany's volume of trade. Typical TBML methods identified included the over- and under-invoicing of goods and services, multiple billing of goods and services, fictitious trades, the use of shell companies, and the investment of incriminated cash in high-priced goods (e.g., vehicles, watches, jewellery, gold, real estate, art). In these cases, cooperation with the private sector and the resulting reporting behaviour of the obligated parties played a decisive role in building understanding of TBML risk.

Germany's experience of integrating knowledge and information from the private sector, particularly FIs, was to ensure the FIs – in addition to the documents required in any case – have sufficient knowledge of the underlying trade transaction and the trading partners. The FIs, particularly the banking sector, are then able to better detect indications of TBML and submit a STR to the FIU.

Source: Germany

60. Nearly all public sector respondents noted they had specifically referenced TBML in their NRAs or were aware of the risk of TBML exploitation through their financial and trade systems and/or via abuse of legal entities in their country. Several delegations referenced TBML as an elevated high-risk [see Box 4.2].

Box 4.2. U.S. NRA and TBML

In the context of its national risk assessments, the United States classifies TBML as both a threat and vulnerability. Threats like Mexican and European transnational criminal organizations (TCOs) and their associated drug trafficking activity, employ TBML schemes because their sophistication makes it difficult for authorities to detect. Vulnerabilities, such as the U.S. financial and trade sectors, are being exploited for TBML purposes.

As early as 2005, the U.S. highlighted TBML in its National Money Laundering Threat Assessment. The 2015 National Money Laundering Risk Assessment (NMLRA) provided an update on TBML schemes, finding most cases involved a complicit merchant or front company in the U.S. that accepted illicit proceeds in exchange for goods. Following publication of this NMLRA, the U.S. Treasury engaged in outreach with various financial institutions across the United States to discuss these findings.

In 2018, the U.S. issued its first National Illicit Finance Strategy[16] and an updated NMLRA. The 2018 reports noted that TBML continued to be a key laundering method associated with drug trafficking and cartels, involving the use of illicit proceeds to buy goods for export. These reports also highlighted the increased use of TBML by PMLs

[16] Available at https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf

and how it can break the link between the predicate crime and related money laundering, making it difficult to associate drug traffickers with the ML activity.

Finally, the 2020 National Illicit Finance Strategy noted that TCOs are relying more on Asian PMLs who serve as money brokers in traditional TBML schemes. TBML was also highlighted as a possible explanation for a steady decrease in the number of bulk cash seizures throughout the U.S. The decrease in seizures could indicate that TCOs are increasing their use of more discreet methods of moving illicit money, such as TBML.

Source: The United States

61. A small number of delegations noted their NRAs does not reflect TBML at all, primarily because they do not consider it a major risk. One contributor was still able to provide insight into its experiences of TBML, despite it not being referenced in the NRA, while two other respondents referenced TBML in the context of general economic crime risks, including legal entity exploitation and the role played by intermediaries, such as company formation agents or financial advisors.

62. Many private sector contributors also undertook their own internal risk assessments to gauge their exposure to TBML or TBTF. In fact, all private sector respondents recognised their exposure to TBML, both in terms of financial products or services offered, and the extent to which their customers may be actively or unwittingly facilitating TBML.

Box 4.3. Example of a private institution assessing its exposure to TBML

Singapore has identified TBML as a priority risk, and the Monetary Authority of Singapore (MAS) has worked to raise industry awareness of the risk over the past few years.

For instance, a FI in Singapore, which has an international presence and global trade links, has identified TBML as a key risk, due to the prominence of trade in Singapore's economy. The institution has assessed its trade finance business to be of higher inherent ML risk based on geography, product, and transaction risk.

To enhance its ability to detect TBML and other risks, the institution plans to roll out an automated transaction monitoring system. It will use data and network analytics to flag higher-risk customers for investigation, removing the need for manual review of individual trade transactions.

Source: Singapore

63. Having identified and understood their risk exposure, FATF Recommendations require jurisdictions to use that insight to inform mitigating actions and drive effective cooperation across its AML/CFT system. For example, jurisdictions should adopt a risk-based approach to supervision and in the context of TBML, this might mean FIs with large trade finance divisions or significant cross-border payment activity require additional oversight from supervisory bodies to ensure the effectiveness of any threat mitigation strategy. Jurisdictions with specialist company formation sectors, in addition to accountancy service providers, should also consider the potential for these firms to be exposed to TBML or TBTF, again ensuring the robustness of any threat mitigation strategy.

Box 4.4. Strengthening DPMS regulation

Following conclusion of the German NRA and input from DNFBP supervision activity, DPMS in Germany were highly susceptible to ML exploitation, including TBML. German authorities noted significant cash payments, just under the due diligence threshold of €10,000. In addressing this risk, as part of transposing the Fourth EU ML Directive into national law, the cash threshold requiring DPMS traders to conduct due diligence was lowered to €2,000.

Source: Germany

4.2. Economic sectors and products vulnerable to TBML activity

64. This section briefly describes the common economic sectors and products at risk of TBML. This should not be considered a definitive list and is primarily provided to give a snapshot of the current risk, while highlighting the diversity of the sectors and products exploited. As one private sector respondent noted, criminals exploit sectors, products, or businesses prone to gaps in, or the inconsistent application of, customer due diligence and know your customer processes across jurisdictions, which can be exacerbated by a nascent or limited understanding of TBML risk.

65. A wide range of economic sectors are vulnerable to TBML, meaning both high-value, low-volume sectors or products (such as precious metals) and low-value, high-volume sectors or products (such as second-hand textiles) can be exploited by criminals to launder the proceeds of crime. Despite this variety in sectors, a handful of common themes conducive to TBML exploitation were identified:

- Goods with wide pricing margins;
- Goods with extended trade cycles (i.e., shipping across multiple jurisdictions);
- Goods which are difficult for customs authorities to examine.

66. Supply chains moving lower-value goods are most at risk to end-to end ownership by a criminal organisation or PML network. The set-up costs can be considerably lower than supply chains moving higher-value goods and may not attract the same level of scrutiny by authorities across the supply chain. An additional benefit of exploiting these products is the scope for supplying multiple markets across different jurisdictions[17]. This also helps mitigate the risk of alerting authorities or regulated firms to any suspicions of market saturation – e.g. it wouldn't necessarily be suspicious if a particular lower-value product, such as clothing, is repeatedly shipped to the same destination.

67. These factors create a suitable environment for the continued use of common TBML techniques. For example, a criminal organisation may execute legitimate shipments of cosmetic goods, creating enough valid documentation to allow for subsequent phantom shipments and misuse of that previous documentation. In some instances, the transactions remained entirely legitimate (so none of the common TBML techniques were used), but the product shipped had almost no value as a saleable good and is literally dumped once it arrived – e.g. second-hand textiles.

[17] These products are also usually in high demand – for example, cheap clothing – which can create the veneer of legitimacy for a TBML network.

68. When OCGs or PMLs exploit higher value products, they are more likely to do so through the penetration and subsequent misuse of established supply chains. OCGs or PMLs may leverage an existing company struggling with a cash flow problem, they buy their way in as a 'silent partner' and use the business and its supply chain contacts to launder the proceeds of crime. This infiltration of legitimate businesses is covered in further detail below.

4.2.1. Gold, precious metals, and minerals

69. The exploitation of gold and other precious metals and minerals is often a factor in TBML schemes, including the use of gold as an alternative form of value within the ML process – i.e. not just a commodity to exploit in moving value, but also a proxy for cash.

70. The association with illegal mining activity creates additional issues such as systematic breaches of health and safety standards, other forms of worker exploitation, and substantial environmental problems.

Box 4.5. Use of gold in a TBML scheme

In the United States, four Peruvian nationals were indicted for their alleged involvement in a multi-billion dollar, international gold ML scheme.

Between 2013 and 2017, the individuals conspired to purchase billions of dollars of criminally derived gold from Latin America and the Caribbean, which they likely knew was the proceeds of criminal activity, including illegal mining, foreign bribery, and illicit smuggling. They used a Florida based company that operated as a dealer in precious metals.

The gold was subsequently sold to complicit U.S. refineries, who completed the ML cycle by paying for the gold, via wire transfers that outwardly appeared to be legitimate payments for wholesale gold purchases.

Source: The United States

4.2.2. Auto parts and vehicles

71. The exploitation of auto parts or vehicles, including trade in second-hand cars or luxury vehicles, was seen in numerous TBML schemes. One scheme included the transportation of damaged cars from one jurisdiction to another, with a legitimate market in place for onward sale, following repair of the vehicle.

72. The OCGs were appropriately declaring the right price at the point of export but were declaring a considerably lower value at transhipment points. This was despite the market for damaged cars being relatively transparent and the sale of vehicles close to their undamaged price. To further frustrate LEAs, the OCG routed payments through an entirely different network of companies located in alternate jurisdictions.

73. The following case study demonstrates how criminals add layering and complexity to their TBML schemes. The OCG exploited several different sectors, including high-end vehicles and lower-value textiles, diversifying their risk exposure and extending their network into multiple jurisdictions.

Box 4.6. Use of vehicles in a TBML scheme

A joint investigation involving Spanish and Italian authorities identified Italian nationals living in Spain who created a network of companies to launder the proceeds of drug trafficking and tax fraud. The scheme had links to Mafia activity.

Having used criminal cash to purchase luxury vehicles in Germany, the OCG also registered and used legal entities and established a fake paper trail for sales and purchases to create value-added tax chains. They then exploited the trade process to both disguise the proceeds of their original criminality and generate additional criminal proceeds. This part of the ML scheme developed to such an extent, the OCG convinced a legitimate supplier in Italy to annually deliver large numbers of vehicles, increasing the legitimisation of their laundering activities.

Alongside the exploitation of these high-end motor vehicles, the OCG also used import/export companies they controlled to purchase other luxury items, such as watches, and lower-value items such as shoes and fabric. The watches were purchased in Spain and Switzerland before being supplied to drug traffickers in Morocco and the Netherlands, while the clothing was purchased in Hong Kong, China and China, before being exported to Colombia and Morocco for onward sale.

Intervention activity in 2017 identified assets worth €8 million across several European countries, while follow-up action in 2018 identified additional assets, including 11 properties, 6 vehicles, 32 bank accounts, and shares of two companies that were all seized.

Source: Europol

4.2.3. Agricultural products and foodstuffs

74. The exploitation of agricultural products, including the abuse of food supply chains involving highly perishable items such as fresh fruit and vegetables, were also noted in TBML schemes. These are a good example of low-value, high-volume products that are not necessarily affected by market saturation given their perishability.

75. OCGs and PMLs penetrate these legitimate supply chains and use them as a means of introducing illicit cash into the financial system. They do not use any of the common TBML techniques, instead they exploit these legitimate supply chains to move their criminal proceeds to different jurisdictions. The following case study highlights the value of joint investigation teams targeting an OCG and PML network exploiting low-value foodstuffs. It also shows how the PML involved third-party invoice settlement to add further complexity to the TBML scheme.

Box 4.7. Use of agricultural products in a TBML scheme

France, Belgium, and the Netherlands launched a multi-agency investigation in 2016 following a routine vehicle check that uncovered EUR €300,000. A joint investigation team was established, focusing on the laundering of the proceeds of drug smuggling.

The drug traffickers employed the services of a PML network that used several different techniques, including TBML. It had been active for an estimated four years and was

suspected of laundering about €400 million. The PML network used underground banking networks in France and Belgium, which collected and remitted the criminal proceeds. The Netherlands-based underground banker worked in an import/export business, trading in foodstuffs with North African countries.

Potatoes and onions were purchased in the Netherlands and Germany, and subsequently exported to several companies in North Africa. These companies were directed to pay invoices into bank accounts controlled by the drug traffickers.

At the end of the investigation in 2019, sentences for ML and drug trafficking were handed down, including the seizure of €4.8 million worth of assets and over €7 million in cash.

Source: Europol

4.2.4. Clothing and second-hand textiles

76. As with foodstuffs, clothing and second-hand textiles are a compelling example of a low-value, high-volume product that allows for an extended supply chain, making them attractive for exploitation in TBML schemes. The extreme price variability also makes it attractive in terms of mis-description of the price to support the laundering activity.

77. Several FIs noted the use of this sector, and one PPP has put together an industry-wide alert highlighting key risk issues linked to the supply of second-hand clothing and textiles.

4.2.5. Portable electronics (mobile phones, laptops, etc.)

78. Portable or handheld electronics are also attractive in TBML schemes as they can be deliberately misrepresented and incorrectly valued, increasing the opportunity to move significant criminal proceeds. The following case study highlights the exploitation of portable electronics by OCGs.

Box 4.8. Use of high-end electronics in a TBML scheme

In 2017, the Australian Border Force (ABF) commenced examination of a TBML referral from an international partner relating to the exploitation of trade in small portable electronics.

Detailed examination through a range of analytical techniques, supplemented by financial and criminal intelligence, enabled ABF specialists to prepare a detailed criminal network assessment of associated entities. Piecing together an extensive network of ML facilitators, the ABF found more than AUD $500 million [EUR €303.6 million] had passed through Australian bank accounts since 2014.

Proceeds were generated by the sale of drugs in North America. The criminal proceeds were transmitted to bank accounts in South East Asia, before they were subsequently layered through a multitude of Australian bank accounts in Australian FIs. The proceeds were remitted to offshore bank accounts, or used to purchase small, high-end electronic devices for export to companies in South East Asia and the Middle East. The undervaluation of exported devices exaggerated the illicit value being transferred offshore.

In this case, the ABF were able to use a combination of automated and manual trade data discrepancy analysis techniques to better identify and assess suspected instances of TBML. Declarations of goods on export from country A should match the corresponding import to country B (because the consignment, in theory, is the same thing). When they did not match in this case, ABF officers had reason to believe that the discrepancies were an indicator of trade mis-invoicing, and therefore, potential TBML. Further investigation and collaboration with partner agencies have enabled the linking of the OCG with the transactions.

Source: Australia

79. In addition to the sectors and products mentioned above, TBML exploitation was also noted in the following sectors: construction materials (lumber), plant machinery, scrap metal dealers, fuel and energy products, and alcoholic or soft drinks.

4.3. Types of businesses at risk of TBML

80. As with sectors, the types of businesses at risk of TBML exploitation are varied. Small- or medium-sized businesses featured in multiple TBML schemes, but some investigations involved large multinational companies, often through overseas subsidiaries that have more fluid trading relationships in distributing products into newer markets. Specific business indicators to note include:

- Rapid growth of newly formed companies into existing markets;
- Evidence of consistent and significant cash payments, including those directed towards previously unknown third-parties. These businesses may also receive unexplained third-party payments;
- Unnecessarily complicated and complex supply chains, involving multiple transhipments;
- Previously established companies specialising in one sector that unexpectedly pivot into an entirely unrelated sector. One example provided noted an IT company

quickly established a foothold in the acquisition and distribution of bulk pharmaceuticals;

- Companies simultaneously involved in more than one unrelated sector.

81. It is important to note that if a company meets one or more of the above risk indicators it does not mean it is being used in a TBML scheme. Further analysis is recommended to offset the risk of false positives, for example, general trading companies that trade in a multitude of commodities.

82. The below sub-sections provide additional insight into several categories of private sector entities that are involved in international trade and may be uniquely positioned to identify TBML, like freight forwarders and customs brokers, or are commonly used by criminals as a tool in TBML schemes, like shell and front companies, while the role of FIs and DNFBPs is explained in Section 6.

4.3.1. Shell and front companies

83. The exploitation of shell and front companies has become a key feature of many different types of ML activity, as well as facilitating a significant number of predicate offences. While there is often a significant intersection between TBML/TF schemes and the exploitation of shell or front companies, they do not feature in all TBML/TF schemes, particularly those involving exploitation of legitimate supply chains.

84. However, some OCGs, PMLs and terrorist financiers do construct their TBML scheme around shell companies or involve them as part of the financial settlement process, anonymising the ultimate beneficial owner to maximum effect. In turn, front companies offer convenient opportunities to integrate physical cash into a business and then exploit its banking relationships to move the cash across jurisdictions.

4.3.2. Freight forwarders and customs brokers

85. Freight forwarders play an important role in facilitating goods shipments, helping buyers and sellers navigate often complex customs and shipping routines and processes. They act as experts in determining the most efficient transportation method in moving the goods, which can incorporate multiple modes for a single shipment.

86. As such, freight forwarders can access and review relevant documentation that might contain indications of TBML, including:

- **Commercial invoices** – although there is no standardised format, the document must include information such as the parties involved in the transaction, the goods being transported and the harmonised commodity description and coding system[18]. A commercial invoice can include a statement certifying the invoice is true.
- **The bill of lading** – is a document issued by a carrier, or its agent, to acknowledge receipt of cargo for shipment. It serves three main functions:
  - It is a conclusive receipt, acknowledging goods have been loaded.
  - It contains or evidences the terms of the contract of the carriage.

[18] This is known as the harmonised system, which is an internationally standardised system of names and numbers to classify traded products. It is organised logically – i.e. animals and animal products are found in one section, while machinery and mechanical appliances are found in another.

- It serves as a document of title to the goods. Simply, it confers title over the goods to the named consignee or lawful holder.

87. Similarly, customs brokers, which can be affiliated with freight forwarders or work independently, work to make the import and export of goods run smoothly, by facilitating the clearance of goods through customs processes. The broker will work with importers to check any necessary documentation or licences are in place, while ensuring the correct duty and taxes are paid, to reduce any delays. Their services can include any or all the following:

- Checking the classification and valuation of goods, ensuring the right commodity codes are used.
- Liaising with government agencies and customs authorities.
- Advising on any necessary licences for import of restricted or hazardous goods.
- Helping arrange correct payment of import duties and VAT as necessary.

88. Even though most jurisdictions do not impose AML/CFT obligations on freight forwarders and customs brokers, they can hold important trade data that can complement information held by competent authorities and FIs in detecting TBML. This is an important consideration as a key challenge in tackling TBML is the disaggregation of relevant data – i.e. that no single stakeholder has ownership of or access to information that would assist in identifying TBML.

89. Competent authorities should consider routine engagement with these critical international trade facilitators to share information and risk indicators to better educate them about TBML/TF schemes. This could extend to establishing new or extending membership of existing TBML-focused PPPs to include freight forwarders or customs brokers.

4.4. Common TBML techniques

90. The FATF 2006 report identified several techniques that form the foundation of TBML:

- ***Over- and under- invoicing of goods and services:*** The key element of this technique is the misrepresentation of the price of the good or service, in order to transfer value. In this type of arrangement, the critical enabling aspect is that the importer and exporter are complicit in the misrepresentation.
- ***Over- and under- shipment of goods and services:*** As above, this involves the misrepresentation of the quantity of goods or services, including 'phantom shipments' where no product is moved at all. Again, it relies on collusion between the importer and exporter.
- ***Multiple invoicing of goods and services:*** This doesn't require the misrepresentation of the price; rather it centres on the reuse of existing documentation to justify multiple payments for the same shipment of goods or delivery of services. Criminals or terrorist financiers exploit this further by reusing these documents across multiple FIs, making it difficult for one institution to identify it.
- ***Falsely described goods and services***: This involves the misrepresentation of the quality or type of a good or service, such as the shipment of a relatively inexpensive good, which is described as a more expensive item, or an entirely different item, to justify value movement.

91. While these techniques are listed independently, in practice criminals can mix these methods in one scheme, further complicating the transaction chain. For example, more sophisticated ML networks may use phantom shipping in conjunction with multiple invoices. One shipment may involve the movement of actual goods to create a veneer of legitimacy, or to test customs compliance processes, with subsequent trading may uses multiple invoices for phantom shipments, serving as a cover for the transfer of funds.

92. Another traditional type of TBML is ***Black Market Peso Exchange (BMPE)***, which has been used by Central and South American drug cartels to launder drug proceeds generated in the United States. One of the drivers behind this scheme is currency restrictions, limiting the ability of legitimate companies to purchase goods from external suppliers. Due to these limitations, businesses have to rely on complicit money traders to exchange legitimate local currency for US dollars. Drug cartels use this chain to move illicit US dollars from one jurisdiction to another.

93. Usually in BMPE schemes, the broker takes receipt of the dollars from the drug cartel's network of cash controllers and uses them to pay the US supplier. Depending on the complexity of the scheme, the broker can pay to the supplier directly, or may place the cash into multiple bank accounts using structured deposits and then forward these funds to the suppliers via wire transfers. The US supplier then exports the goods to the companies in the Central or South American country, which then transfer local currency to the local money broker. After that, the money broker passes local currency to the drug cartel, minus commission. This scheme ensures no cash is moved between the jurisdictions, where it may be identified and intercepted by LEAs.

94. The case study below highlights a scheme involving BMPE, reinforcing the fact that such schemes involve a degree of knowledge by the importer and exporter about the illicit origin of the funds.

Box 4.9. BMPE Scheme

In January 2020, the US Justice Department indicted six Colombian nationals, in cooperation with an Indian national, for their roles in an international money laundering scheme involving TBML and the use of unlicensed money transmission business.

The purpose of the scheme was to launder the proceeds of drug trafficking, primarily using a BMPE-style process so the cash located in the United States was not physically transferred.

The scheme was built around the Colombian nationals allegedly working as money brokers that receive criminal proceeds from couriers located throughout the United States, and the receipt of incoming international wire transfers. The physical cash was introduced into the U.S. financial system so as not to raise suspicion, before being transferred to the business bank account controlled by the Indian national, who was an alleged complicit merchant. The merchant exported consumer electronics to buyers throughout the world, including importers located in Colombia.

The merchant exported roughly the equivalent value of consumer products to the importers in Colombia, who in turn arranged to pay for the products by delivering pesos to the money brokers in Colombia, who passed this to the drug trafficking organisation. This negated the need for the drug traffickers to attempt any movement of cash across borders, thus reducing their risk of detection.

The case study also highlights the continued reliance on peso exchange mechanisms and the misuse of legitimate trading relationships by complicit exporters and importers to move the equivalent value from the United States to Colombia.

Source: The Unites States

95. Overall, a key finding from the insight generated across the FATF Global Network, FIUs and the private sector is that these techniques are still prevalent today. However, other trends are emerging, including the exploitation of legitimate supply chains that operate without the collusion between importer and exporter, or the introduction of criminal cash into trade transactions, including the growth of surrogate shopping.

4.5. Assessment of current TBML risks

96. The continued use of these common TBML techniques is complemented by the consolidation of previous methods of financial settlement (e.g. third-party invoice settlement) and the growth of newer techniques that support the integration of cash into the financial system. Some of these methods do not rely on the techniques of product or trade document misrepresentation.

- **Illicit cash integration –** given the prevalence of TBML as a process for laundering the proceeds of illegally smuggled commodities, OCGs and PMLs need a way of successfully integrating illicit cash into the financial system, including the exploitation of other types of FI. The report has already covered how this works in traditional BMPE schemes, there is variation of this method whereby OCGs or PMLs looking to dispose of illicit cash cooperate with other OCGs or PMLs looking for cash. Another variation of illicit cash integration is the exploitation of surrogate shopping networks and the infiltration of legitimate supply chains.

- **Third-party intermediaries facilitating invoice settlement** – this was first identified in the 2006 report and has remained a constant feature of TBML schemes, including those schemes not involving complicit relationships between the importer and exporter. As this report is targeted at a broader audience, this risk is revisited here to help educate and inform those who may find they are being told to engage with an entirely unknown and unrelated third-party in settling the invoice.

4.5.1. Illicit cash integration

Exploitation of other types of FIs

97. While a substantial amount of TBML cash integration involved banks, OCGs and PMLs can also exploit other types of FIs, including money value transfer services (MVTS) or informal mechanisms like hawala. For example, conspirators involved in a false invoicing TBML scheme have used MVTS to facilitate payment for the goods, rather than attempt payment via a bank. The OCGs or PMLs perceive the MVTS sector[19] to have a less developed understanding of TBML, so the MVTS wouldn't question why it is facilitating a business payment of a significant amount rather than the payee using a more appropriate method.

98. This reinforces the requirements set out in the FATF Recommendations, which set out obligations on customer due diligence and MVTS respectively. Supervisors and regulators should consider whether these businesses need to establish specific TBML/TF risk mitigation policies and controls in meeting their AML/CFT requirements.

Offsetting schemes

99. A variation of BMPE is called **offsetting or compensation**, whereby OCGs or PMLs dispose of illicit cash by cooperating with OCGs or PMLs looking for cash. The following case study highlights how these different groups cooperate to manage illicit cash integration through a hybrid TBML and SBML scheme.

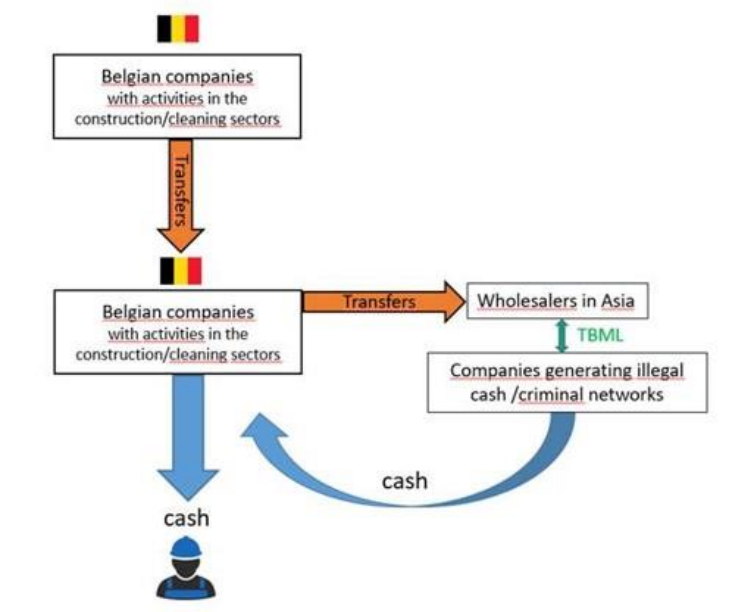
[19] Some PMLs are known to operate or have a close relationship with MSBs, ensuring they retain control of the payment process.

Box 4.10. Compensation scheme

For several years, Belgian authorities have noted that Brazilian or Portuguese nationals are setting up or taking over Belgian companies in the construction or cleaning industry.

These companies are often used as a cover to employ non-declared workers in Belgium, operating as part of a network of different companies, all with the same profile that establish and exist for a limited time – essentially to carry out specific transactions.

They can be quickly and effectively replaced by new companies, with new managers, in order to perpetuate the system. These companies take receipt of criminal cash from other criminal networks, providing a veneer of legitimacy by invoicing for building maintenance services; the funds are then transferred to wholesalers in Asia. The wholesalers are instructed to purchase merchandise on behalf of Belgian retailers, which is subsequently imported and sold as part of a related TBML scheme.



Source: Belgium

Surrogate shopping networks

100. Surrogate shopping networks involve individuals or networks of shoppers purchasing desired goods on behalf of wealthier individuals, ostensibly to circumvent customs controls or other forms of tariff restrictions. Some shoppers may also make purchases on behalf of OCGs to distance them from the asset, suggesting the surrogate shopper has at least some knowledge that what they are doing is on behalf of an OCG. This type of activity has been exploited as part of TBML schemes and there are similarities with BMPE, whereby OCGs or PMLs provide local currency (the proceeds of crime) to these surrogate shoppers, who pay for desirable goods that are transported to another jurisdiction and passed to the OCG or PML.

101. An adaptation of this scheme involves the surrogate shopper paying for the requested goods using credit cards, and the OCG or PML settling their debt using the proceeds of crime. For example, students were making multiple purchases of portable electronics, such as smart phones and tablets. Their credit card balances were subsequently

settled via electronic funds from companies suspected of laundering the proceeds of drug trafficking. Not only did this allow for the laundering of criminal proceeds, but the electronics were suspected of being sent for onward sale into grey markets in Asia and the Middle East. This process can be used with the traditional TBML techniques, including the misrepresentation of the goods purchased, to increase the margins of the proceeds of crime transferred as payment.

Infiltration of legitimate supply chains

102. In this case, an OCG or PML purchases a stake in a legitimate business, which may or may not be struggling financially, and continues using its supply chain as a method of integrating illicit cash into the financial system. The OCGs or PMLs do not attempt to change the business practices of the company they've invested in, nor do they necessarily introduced any of the common TBML techniques referenced previously. Instead, their aim is a slow and steady increase of introducing illicit cash into the business, while maintaining those existing supply chain relationships.

103. This method presents challenges for authorities or FIs to detect the TBML scheme, however, as evidenced in the case study in Box 4.6, it still is possible to investigate seizures of illicit cash and uncover a sophisticated TBML scheme.

4.5.2. Third-party intermediaries facilitating invoice settlement

104. Third-party intermediaries have remained a constant feature of TBML schemes, since they were noted in the 2006 report. They often appear as part of the invoice settlement process, and are often associated with the exploitation of open account trading, because of the lack of oversight by FIs. They can serve a dual purpose, depending on where in the chain the OCG or PML is involved.

105. For example, in penetrating legitimate supply chains and sourcing goods without any misrepresentation, the OCG may pay for those goods by involving a previously unknown third-party (usually the company responsible for integrating criminal cash) into the transaction. As noted in the section on shell or front companies, these third-parties may be based in locations with beneficial ownership secrecy provisions.

106. While FIs appear to be generally aware of the risk of these third-parties settling invoices, unsuspecting firms receiving payment may not question why their trade relationship has suddenly expanded to incorporate a previously unknown third-party, who may be based in a different jurisdiction.

107. Even though it is a long-standing risk linked to TBML schemes, it is not systematically reported by DNFBPs, for example by auditors or accountants who may come across such payments. Greater awareness of this technique may increase the frequency of its reporting and the development of improved intervention strategies to disrupt TBML schemes. The following case study highlights the role of third-party intermediaries and the abuse of shell companies as part of an extensive TBML scheme.

Box 4.11. Third-party settlements

The New Zealand FIU (NZFIU) received multiple SARs regarding payments to New Zealand fruit export companies which were being made from bank accounts in Eastern Europe, which were registered to shell companies based in high-risk jurisdictions. SAR reporting showed the New Zealand companies received approximately $1.5 million during an 18-month period from these overseas accounts.

NZFIU enquiries established that the transfers to the NZ companies were payments for legitimate exports of NZ fruit to a South-East Asian jurisdiction. When questioned, the company representatives could not explain why the payments were originating from shell company accounts, which had no known relation to the company actually receiving the exported goods.

The New Zealand banks processing the payments suppled the FIU with invoices which were provided to them as justification for the payments – these invoices were clearly fraudulent and depicted the transactions as payments for export of 'ceramic tiles' from the New Zealand company to a company in Eastern Europe. The invoices were 'signed' by the purported manager of the NZ company, but enquiries determined there was no one by that name employed at the company.

The NZFIU assessed these payments, (potentially in the tens of millions of dollars, based on the high-volume of account activity) formed part of a complex TBML scheme being operated out of Eastern Europe, in which illicit funds were converted to trade goods and shipped for resale in a different jurisdiction, generating clean funds.

Source: New Zealand

4.6. Trade-based terrorist financing (TBTF)

108. TBTF was only referenced by a handful of respondents, particularly as consideration when developing their NRA, recognising that what made TBML schemes attractive in moving value, offered the same opportunities to terrorist financiers.

109. In practice, TBTF schemes can and do rely on the common TBML techniques. They can also feature legitimate firms and transactions right through the supply chain, until the funds are eventually diverted to terrorist organisations.

110. In the below case example, terrorists used an existing supply chain to move funds from one country to another, avoiding making direct payments to each other and using a commodity as a mean of moving value.

Box 4.12. Misuse of an existing trade chain to move funds for terrorists

Case example 1:

An importer in country A wanted to purchase goods from a supplier in country B as part of the ongoing legitimate trade between them. However, payment for the goods was made by operatives of a terrorist organization located in country C. Once the supplier received the payment, the goods were shipped to the importer. After receiving the shipment, the importer paid the value of the goods in cash to operatives of the same terrorist organisation located in Country A.

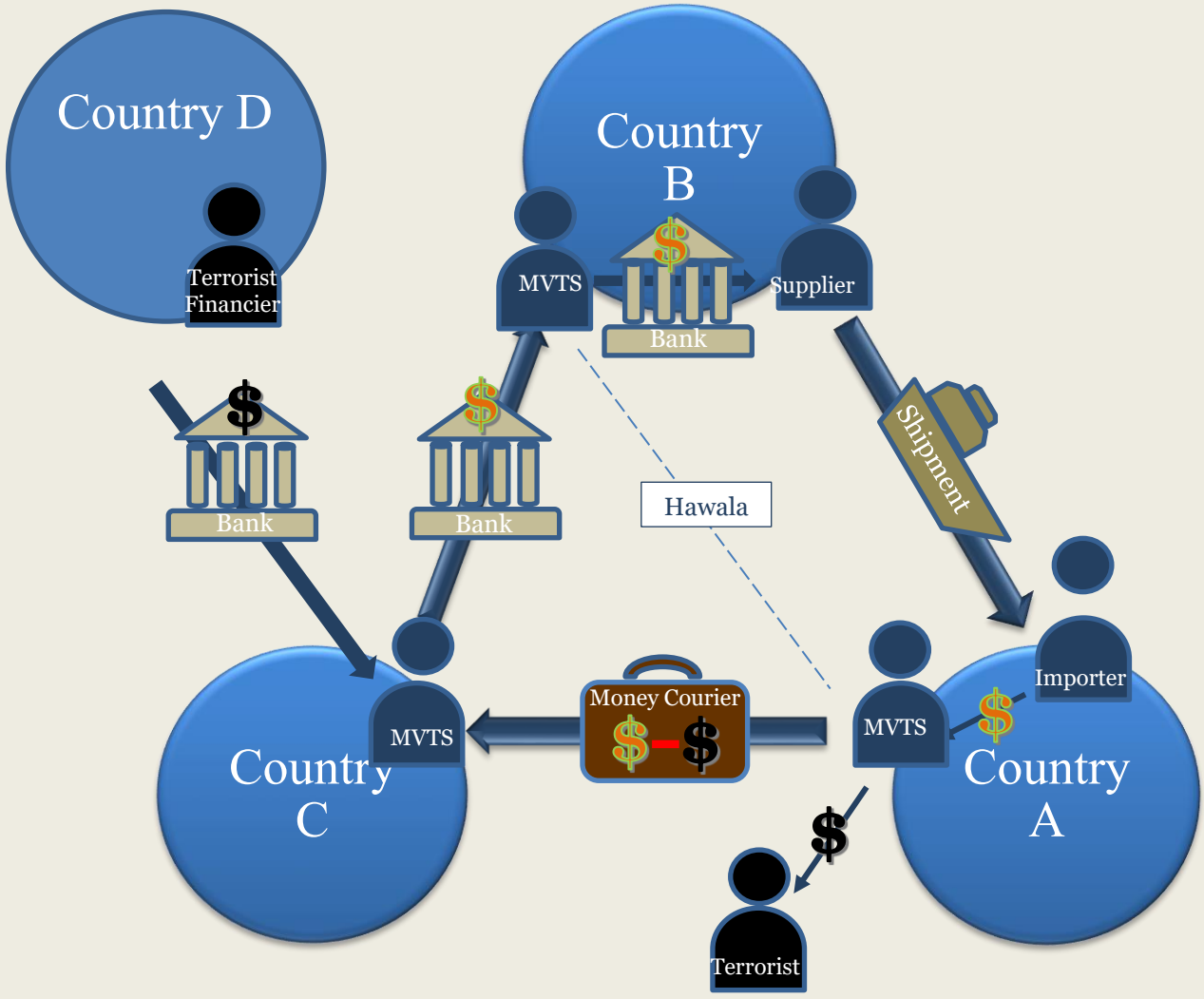
In this way, the terrorist organisation was able to transfer cash from country C to country A through the legitimate trade system by using commodity as currency. The goods were detected by the Israeli Customs Authority and confiscated.

Case example 2:

In another case, a network of MVTS and hawala was used in order to arrange settlements for the trade of goods between importers in Country A and exporters in Country B. The importers paid for shipped goods through a MVTS in Country A, who then transferred the funds to a MVTS in Country B via hawala. The MVTS in County B then transferred the payments to the exporters through a bank. For settlement purposes, the MVTS in Country A sent money through cash couriers to an MVTS in Country C, who then sent a bank transfer to the MVTS in Country B.

A terrorist financier from Country D then used this trade network in order to transfer TF funds to a terrorist organization in Country A. The financier transferred a sum of money to the MVTS in Country C, and this MVTS then transferred the sum to the MVTS in Country B. The same sum was then deducted from the amount, which the MVTS in Country A would have needed to transfer to the MVTS in Country B for settlement purposes. Instead, the MVTS in Country A passed the same sum to a local terrorist organisation.

In this case, the terrorist financier penetrated the trade chain between the supplier and importer, using complicit MVTS to inject funds intended for TF purpose into the trade transactions, while avoiding making direct payments to the terrorist organisation.



Source: Israel

111. In the following example, suspected terrorists used the false invoicing technique to facilitate the transfer of funds to terrorists.

Box 4.13. TBTF case

Italian authorities identified suspicious financial activity in personal and business bank accounts linked to two brothers. The brothers were linked to firms operating in the wholesale and retail motor vehicle trade. The purchase and movement of the vehicles was ostensibly legitimate, however what alerted suspicion was the significant discrepancies in how the economic activity behind the vehicle sales raised suspicion. For example, there were significant cash deposits and withdrawals, plus personal bank accounts credited with monies originating from other commercial entities.

An initial analysis by the Italian authorities suspected a ML network, which was operating a scheme using false invoicing. However, further investigations began to identify identified a link to TF, which was supplemented with open source reporting. Key risk indicators included the jurisdictions linked to the export of the vehicles, the fact these jurisdictions had poor counter-terrorism financing safeguards, and the economic sectors involved, which had been associated with TF activity previously.

This was confirmed through subsequent STRs and the validation of the intelligence by the Italian police. Profits from the transnational car dealing were sent to Middle Eastern import/export companies and onwards to terrorist organisations.

Source: Italy

4.6.1. Services-based money laundering

112. Services-based money laundering (SBML) is not TBML, and is included here for reference as it is recognised as an increasing risk, including through open source reporting[20]. However, the fundamental difference between SBML and TBML is that SBML schemes rely on exploiting the trade in services or other intangibles to disguise and justify the movement of illicit proceeds.

113. While this report does not explore the SBML phenomenon in detail, SBML schemes can create further complexity for competent authorities or regulated entities to successfully detect and disrupt ML. For examples, for services such as consultancy or advisory provision, it is hard to assess the legitimacy of the relationship between service purchaser and service provider. In addition, there is no physical commodity traded, which would normally create import or export data. The following services and sectors were identified as vulnerable to SBML:

- Gambling, particularly online gambling service providers;
- Software providers, including gaming and business software, such as electronic point of sale services;
- Financial services, including virtual asset wealth management;
- Consultancy and advisory services;
- Trademarks and similar intangible items such as intellectual property rights.

[20] Foundation for Defense of Democracies policy brief: Service-based money laundering: The Next Illicit Finance Frontier

5. Challenges to countering TBML

114. Despite significant attention to TBML within the FATF Global Network and a broader expert community, countering this form of ML continues to be challenging for jurisdictions. The aforementioned reports of 2006, 2008, and 2012, as well as the WCO and Egmont Group's Customs-FIU Cooperation Handbook[21] stress TBML as a particularly complex form of ML that causes various difficulties at each stage of the investigative and detection processes. These difficulties, as well as broader challenges to international cooperation and difficulties experienced by the private sector in identifying TBML schemes, have led to a relatively low number of successful TBML investigations across the globe so far. The section below aims to summarise the most critical of the challenges that significantly undermine the effectiveness of measures implemented by jurisdictions to counter TBML.

5.1. Lack of understanding and awareness

115. The FATF TBML publications in 2006 and 2008 put TBML on the radar of agencies worldwide, while the execution of NRAs have contributed to a better understanding of TBML risks across jurisdictions. An increasing number of publications on TBML by other international bodies, academia, and national authorities have also provided valuable insights on TBML, thus contributing to the understanding of this phenomena by the public and private sectors. However, as noted by many respondents, some of the involved authorities still have only a basic understanding of TBML and may not be aware of more sophisticated aspects of this crime. For the authorities that have an advanced understanding of TBML, it is an ongoing challenge to keep pace with the evolving TBML risks. As authorities increase their knowledge of TBML and take efforts to adjust measures to combat it more effectively, criminals are constantly seeking new opportunities to legitimise criminal proceeds through the misuse of the international trade system.

116. One of the factors underlying these challenges is the relative complexity of TBML schemes. They can involve a multitude of sectors and commodities exploited as a means of moving value, from second- hand cars to flowers, meaning no one scheme is like another. Moreover, law-abiding organisations involved in the supply chain, like production companies and traders, see a piece of the puzzle, but not all of them are sufficiently aware of the signs of TBML. They may accordingly overlook such activity, even if they have the sophistication to detect it. This, in turn, makes it difficult for authorities to identify higher-risk sectors and prioritize their actions to mitigate the risks.

117. A growing number of online business opportunities has opened new horizons for international trade. At the same time, it has also created additional challenges to the understanding of TBML methods, and technologies used by public authorities for oversight and analysis of trade transactions may not be keeping pace. New technologies and the digitalisation of trade allow for an increased speed of trade operations, which in turn requires authorities to adopt their strategies and develop knowledge not only about the "modi operandi" of criminals, but features of the modern trade system as well. In order to identify suspicious trade and financial transactions among the thousands of legitimate transactions in a timely manner, public authorities also need to digitalize the tools and techniques they apply to analyse financial and trade data.

[21] See the web sites of both organisations for a public version of the hand book.

5.2. Domestic coordination and cooperation

118. Previous studies have highlighted challenges to collaboration between national authorities as one of the most prominent issues in the context of countering TBML. Based on the provided inputs for this reports, a lack of collaboration remains one of the largest concerns across the authorities, hindering the detection and investigation of TBML.

119. The FATF Recommendations require jurisdictions to ensure that their investigators of predicate offences are either able to investigate associated ML themselves or be able to refer the case to another agency for a follow-up parallel financial investigation. However, one of the factors associated with this challenge is that investigative authorities still could be focused on predicate offences and de-prioritise investigations into ML, including TBML, especially if it's not their primary function. For example, the police may prioritise investigation of predicate offences, tax authorities may be primarily focused on tax fraud and customs authorities on commercial trade fraud and smuggling, while ML may be seen as a lower priority.

120. Since TBML is based on exploiting vulnerabilities of the trade system, some of its material elements may be similar to other trade-based crimes. This similarity may lead to a mischaracterization of the identified scheme by authorities as smuggling or fraud, instead of TBML. For example, if authorities detect a discrepancy in the documentation accompanying the cargo, they may prefer to stop the shipment and charge the carrier with customs fraud or a violation of intellectual property rights without investigating whether this could be TBML.

121. As recognised in the FATF Recommendations, domestic coordination and cooperation is one of the fundamental pillars of an effective AML/CFT regime. In particular, the FATF Recommendations require that policy-makers, FIUs, LEAs, supervisors, and other relevant competent authorities have effective mechanisms in place to cooperate, and, where appropriate, coordinate and exchange information with one another. This standard ensures jurisdictions are able to link the work of authorities responsible for collecting, analysing, and storing different types of data with authorities tasked with investigating predicate offenses and ML.

122. Still, many respondents highlighted a lack of information sharing between national authorities, or ineffective mechanisms for such sharing, as a key challenge in countering TBML. As identified by FATF and FSRB Mutual Evaluation Reports, many of the jurisdictions assessed so far have the necessary legal framework in place allowing the exchange of financial intelligence between a range of authorities, including the FIU and LEAs. However, in some cases low effectiveness of such cooperation does not always allow authorities to detect and investigate ML, including TBML, and confiscate proceeds of crime to a sufficiently high degree.

123. Difficulties with the analysis of and combining tax, trade and financial data by investigators, FIU analysts, and other relevant experts is another frequently noticed challenge. To properly identify TBML activities, authorities often need to analyse and match large volumes of data from various sources, some of which may be held by different agencies, such as customs data, information on STRs, and criminal records. Each agency holding data may store it within its internal IT systems and there may be no information sharing mechanism allowing timely access to this data by other agencies, LEAs, or the FIU. Even if such mechanisms are in place, they may not allow cross-referencing of data from various databases in an automated manner, thus requiring additional time and resource from the involved authorities to manually cross-check and analyse it. For example, financial data reported to FIUs, STRs in particular, and data on imports and export may be stored in unstructured formats or there may be issues with the quality and consistency of reporting.

5.3. International cooperation

124. Providing the appropriate international cooperation in a timely manner is crucial to the effective detection and investigation of any criminal activity that goes beyond one jurisdiction. For TBML, such cooperation is particularly critical, since money launderers often use front companies registered in one jurisdiction and transfer relevant funds and ship goods between others. All of these pieces form a puzzle, which can only be solved if all the involved jurisdictions provide necessary assistance to each other.

125. TBML may take place transnationally, e.g. the predicate offence often takes place in jurisdictions other than the jurisdictions in which the TBML occurs. Hence, to ultimately investigate and prosecute TBML, jurisdictions would heavily rely on effective and working international cooperation channels to ascertain that the predicate offence has taken place.

126. However, jurisdictions continue to experience a lack of effective information sharing, which inhibits their ability to identify and investigate TBML. One challenge is providing information in response to a request of a foreign counterpart without significant delays. Sometimes the delays are due to issues with domestic cooperation within the requested jurisdiction, as the required information may be stored by different authorities, and compiling it into one report may take significant time. In addition, when authorities of one jurisdiction seize goods in response to a request of another jurisdiction, for example when there is a suspicion that the goods are used in a TBML scheme, this requires the importer to pay the additional costs of holding and storing the goods proportionate to the period of the seizure, putting an extra financial burden on the importer.

5.4. Investigation and Prosecution

127. As identified in FATF's 2018 Professional Money Laundering report, TBML is one the methods most preferred by PMLs, and is often combined with the use of front companies[22], front men, and other ML techniques. In professional ML networks, ML activity, including TBML, is carried out by one group of criminals, while the predicate offences are committed by other criminals. Such disconnect between the ML activity and predicate offences can mean that the investigators of the predicate offences (anti-drug trafficking units, anticorruption agencies, etc.) may lack the sufficient expertise to investigate the associated ML activity. For jurisdictions that experience difficulties with domestic cooperation, this would likely lead to charging criminals only with predicate crimes, like drug or human trafficking, and other trade-based crimes, like VAT-fraud, and smuggling.

128. As for any other type of ML, prosecuting TBML requires the need to prove that the laundered funds or assets are the proceeds of crime and that the defendant knew this. The prosecutor may be able to collect enough evidence to prove the objective side of the ML offence, i.e. how the proceeds of crime were converted and transferred, but the knowledge requirement can be particularly hard to meet, even using the factual circumstances of the case as evidence. This is especially the case for third-party ML or if the predicate offence was committed in another jurisdiction. For example, the defendant may state that he/she was not aware of the illicit origin of the funds at the time of their receipt and the prosecution would have to obtain enough evidence proving otherwise. In cases where criminals also misuse legitimate trade operations, illicit and legitimate funds are often mixed together, creating additional challenges for the authorities to identify the laundered property. These

[22] See the joint FATF/Egmont Group "Concealment of Beneficial Ownership" report on further features of shell and front companies.

difficulties, coupled with the overall lack of knowledge and understanding of TBML, often result in the prosecution of predicate offences only, while TBML activity remains out of focus.

5.5. Challenges from the Private Sector perspective

129. According to the FATF Recommendations, certain private sector companies should be obliged to implement a wide range of AML/CFT measures, including client due diligence, record keeping and STR reporting. These measures are designed to limit the ability of criminals to launder funds and other assets and finance terrorism, while ensuring that FIs and DNFBPs have sufficient tools to protect themselves from misuse for ML and TF purposes. Even when a criminal attempts to use the services of these businesses, these tools should allow the involved entities to establish a suspicion of such activity and promptly report it to the FIU.

130. FIs and DNFBPs are often on the forefront of the fight against ML, since they are either involved in moving value (e.g. by executing transactions on behalf of their clients) or they have unique knowledge about their clients' financial activities (e.g. accountants and lawyers). At the same time, being on the front lines against ML and TF creates significant challenges for the private sector, as criminals constantly improve their ML methods and the private sector has to keep pace. It also should be noted that most trade and production chain companies do not have similar reporting obligations under the FATF Recommendations (unless they fall within the scope of business activities defined in the Recommendations, like dealers in precious metals or stones), nor do they typically fall under the domestic legal framework of many jurisdictions, which places the onus on FIs and DNFBPs to detect potential instances of such activities and appropriately advise the FIU by reporting an STR in a timely manner

131. Most private sector respondents, mainly FIs, consider TBML as the hardest type of ML activity to detect. TBML is highly adaptive and can exploit any sector or commodity, making it difficult for FIs to prioritize resources and translate the latest insights into the business rules and compliance systems. In practice, TBML schemes can consist of a large number of front companies, with funds transmitted between several banks, meaning each of the involved FIs can see only a small part of the network. This fragmentation of TBML schemes makes it inevitably difficult for FIs to identify potential TBML schemes based on the analysis of the whole chain, and in many cases limits their ability to detect discrepancies in supplementary documentation and customer profiles.

132. Another challenge faced by FIs is the verification of information provided by their customers. This can be an issue for all types of ML, when a lack of a public registry can present difficulties for FIs trying to verify an address, income, or other client-related data. TBML schemes only exacerbate these challenges. During the due diligence process for a trade transaction, for example, a client might submit a copy of the invoice, contract, or other supplemental documents to the bank to justify the transfer of funds from one jurisdiction to another. If the bank has problems accessing customs data, it will not be able to promptly verify, amongst other things, the authenticity of the documents, whether the goods have been actually shipped, and whether their quantity and description matches the contract.

133. Many TBML techniques require both the buyer and the seller to be complicit, sometimes meaning that the same person or a group of persons execute control over the different parties of a transaction. In this case, obtaining information about the beneficial owners (BO) of the customer's counterparties may assist the FI in detecting TBML. However, such information may not be available, for example if the counterparty has never been a customer of that FI or if there is no public registry of BO information available. The

counterparty may also be incorporated in a jurisdiction other than the one in which the FI executing payment is registered, further complicating the FI's efforts to collect BO information.

134. Another reoccurring challenge faced by FIs in identifying TBML schemes is estimating the "fair price" of a traded commodity. This challenge is particularly relevant for TBML schemes using the over-/and under-pricing technique, in which criminals list a higher or lower price for the traded commodity compared to the usual market prices in an attempt to move additional value under the guise of the trade operation. FIs often have only a vague description of the traded good, and establishing a "fair price" can require significant resources and may be based solely on open source information. In addition, some of the commodities used by criminals are not traded in public markets and there are accordingly no benchmark prices available.

135. Moreover, because TBML involves international trade, the documentation provided to FIs is often in different formats and languages, meaning that verification will likely be done manually. This requires FIs to devote additional time and resources, including hiring highly qualified staff, what may be more difficult for smaller FIs with more limited compliance budgets.

136. In this context, paying methods like letters of credit or documentary collection, which require customers to provide the FI with more documentation than open-account trade, are often seen by the private sector as less vulnerable to TBML. Thus, money launderers may see open account trade as more attractive because the FI has more limited oversight of the transaction. At the same time, even when an FI suspects its customer being involved in TBML and terminates relationships with them, the customer may still be able to open a new account in another bank.

6. Measures and best practices to counter TBML

137. The FATF Recommendations set out a comprehensive framework of AML/CFT measures for jurisdictions to apply in order to counter ML and TF effectively. At the same time, jurisdictions have a certain degree of flexibility in terms of how those measures are translated into the national legal and regulatory frameworks and applied in practice. This flexibility is based on the context, risks, and other structural factors of each jurisdiction.

138. This section aims to summarise some of the existing good practices used to counter TBML, in an effort to help jurisdictions enhance the effectiveness of their AML/CFT measures – while also recognising there is no "one-size-fits-all" approach. Some of the practices listed below may go beyond the measures set out in the FATF Recommendations, but may still be helpful for competent authorities to consider, subject to the composition and features of the domestic AML/CFT framework and ML/TF risks.

139. The reader is also encouraged to refer to the relevant sections of the 2006, 2008, and 2012 studies on TBML for other practices that could be applied to increase the effectiveness of domestic measures to counter TBML.

6.1. Increasing the understanding of TBML

140. As noted in the above sections, building a sufficient level of knowledge of TBML schemes should be the foundation of any strategy to counter this form of ML. From the public sector perspective, this often means identifying and assessing TBML risks present in the jurisdiction, including the economic sectors and financial instruments involved. This enables the public and private sector actors to focus their resources and adjust broader ML

strategy appropriately. However, as noted by many respondents, a lack of knowledge and understanding of TBML schemes is a common challenge not only for the private sector – which may have insufficient resources to follow the most recent AML/CFT developments -- but also for public authorities.

141. Jurisdictions may use different sources of information to develop an understanding of TBML schemes across the public and private sectors. One source is the NRA, as it typically summarises the available information on ML/TF risks present in the jurisdiction, sometimes with a breakdown by specific sectors. Although the NRA should reflect the full spectrum of a jurisdiction's TBML risks and their components, it is likely intended for experts who already have some understanding and knowledge of TBML. Moreover, in some countries the NRA may not be publicly available. Thus additional efforts may be required to make the NRA content available and understandable for a broader audience.

142. While this paper does not aim to provide specific guidance on how jurisdictions or private sector bodies should identify and assess their TBML risks and vulnerabilities, a number of initiatives in various regions have focused on increasing TBML knowledge and improving risk understanding. This includes a number of national and regional experiences, ranging from those providing "basic" knowledge of TBML and focusing on FI customers, to initiatives intended for experts requiring more advanced training. Such initiatives could be driven and framed by different bodies, for example:

- Private sector entity that seeks to raise awareness amongst their customers to minimise the likelihood that they will be involved in a TBML scheme.

Box 6.1. Dutch bank initiative

In the Netherlands, a FI provided all of its business customers with a flyer designed to raise awareness of TBML risks. The flyer included an example of a TBML scheme and an email address if customers had questions regarding TBML and their business.

Source: The Netherlands

- FIUs or other authorities attempting to raise the level and quality of STR reporting from the sectors that are considered vulnerable to TBML.

Box 6.2. Cooperation between FIU and DNFBPs

In 2019, the FIU of Germany provided guidance to DNFBPs and other regulated entities (e.g. auto traders and art/antiquities traders), through a series of regular lectures and engagement through the chamber of industry and trade. This was expected to continue in 2020, while taking into account the COVID-19 pandemic-related restrictions.

The guidance led to a significant increase in the number of registration applications (registration of obliged entities with the FIU), as well as an improvement in the quality of questions raised with the FIU and its representatives at trade fairs and lectures, indicating an improved understanding of ML risks.

The FIU provides DNFBPs, after registration on their website, with typologies and other relevant information about ML prevention and STR reporting. In order to reach traders of goods not yet registered with the FIU, there was also a close dialogue with relevant associations to help raise awareness of ML among their members.

Source: Germany

Box 6.3 Raising FIs' knowledge of TBML

The Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership ("ACIP brings together selected industry participants, regulators, LEAs, and other government entities to collaboratively identify, assess, and mitigate the key ML, TF, and proliferation financing risks faced by Singapore. One of ACIP's working groups focuses on TBML risks, bringing together insights from banks (particularly those with a focus on trade finance), regulators, LEA and professional services organisations. This working group developed an industry best practice paper on the management of TBML/trade financing risks, which also included preventive measures and tips on training and awareness for FIs[23]:

- FIs should provide its staff with relevant, specific, and targeted training to detect and prevent TBML risks and to heighten the awareness of risks and competence of such relevant staff to mitigate ML/TF/PF risks and comply with regulatory requirements.
- FIs should provide training and disseminate information to all relevant staff to highlight significant regulatory changes and new risks and typologies noted for managing TBML risks.
- Training should be refreshed periodically, as determined by the FI's risk assessment; it should be aligned with the FI's policies and procedures; and it should consider circumstances unique to the FI, such as products offered, operational locations, and customer types.

Source: Singapore

[23] https://abs.org.sg/docs/library/best-practices-for-countering-trade-based-money-laundering.pdf

- International bodies providing guidance on TBML as part of their international programs or enhancing cooperation with the private sector.

Box 6.4. Collection of TBML case studies

In July 2020, the Information Exchange Working Group of the Egmont Group (Egmont IEWG) endorsed a Case Book resulting from the Project "Conclusions from large scale cross-border money laundering schemes". The project aims to initiate the discussion and development of possible approaches to identify networks, patterns and indicators for large scale cross-border money laundering schemes by pooling FIUs' insights findings derived from past "Laundromats".

Drawing back on the diverse expertise and experiences of FIUs on detecting and analysing large scale cross-border money laundering schemes, one of the project's work streams was dedicated to gathering relevant case studies. Different FIUs observed that in such schemes criminals were widely applying TBML techniques to disguise and move the proceeds of crime. Hence, the case collection was carried out with a dedicated focus on TBML-schemes and the use of different TBML techniques. In total, more than 20 FIUs contributed to this work stream, allowing to develop a collection of diverse TBML case studies compiled in the "Case Book", demonstrating how the international trade system could be misused by criminals for ML purposes.

The "Case Book" is available for FIUs on the Egmont Group's secure web-site. Other domestic competent authorities and selected reporting entities can access it via their respective FIU.

Source: Egmont IEWG

Box 6.5. Europol Financial Intelligence Public Private Partnership (EFIPPP)

The EFIPPP is the first transnational information sharing mechanism established in the field of Anti-Money Laundering and Counter-Terrorist Financing. It was launched in December 2017 as a pilot project of Europol-Institute of International Finance High Level Project of Law Enforcement, Regulatory and Banking Sector. It aims to create a platform for the exchange of information among trusted partners across national and sectorial lines. It provides practical input (e.g. typologies) aiming at refining the Suspicious Transaction Reporting efforts, moving from a compliance-led to an intelligence-led approach.

EFIPPP brings together law enforcement agencies, financial intelligence units and/or regulatory authorities from 11 EU member states, 4 third countries to the EU, 25 financial institutions with an international footprint, EU institutions and organisations, one international organisation as well as various civil society organisations and research institute as observers. The EFIPPP is triggering growing interest: from 15 financial institutions and 6 participating countries in 2017 to 25 financial institutions and 15 countries today. A new governance model has been very recently been adopted and is currently being implemented to structure the growth and the priorities of the EFIPPP in the coming years. Members meet on a quarterly basis and in dedicated working groups and continuously exchange through a dedicated platform for experts.

Past work on TBML in typologies drafted by the EFIPPP has been linked to drug trafficking and VAT fraud. The typology focuses on the created interrelation between drug related offences (production, cultivation, smuggling and distribution), money laundering and tax fraud.

Source: Europol

Box 6.6. ADB experience with TBML

In 2019, the Asian Development Bank (ADB) published a brief effective practices paper examining AML/CFT compliance in trade finance operations. The paper provides a practical understanding of trade finance and how these departments work in commercial banks.

In addition, ADB is also working with a number of public and private sector stakeholders, using the proposals made in the APG's 2012 report, to address challenges with the quality and integration of trade data to improve detection of TBML. The Singapore AML/CFT workshop held in March 2019 led to the development of trade data points that could be factored into existing or emerging feedback loops between the public and private sector. Those trade data points are intended to be used by authorities and private sector entities to improve the quality of STR reporting. They may include greater specificity on the TBML technique identified, key information on trade transaction counterparties, and details of the transaction and transport methods.

Applying this type of approach through a PPP can also help bring together relevant data holders, broaden the picture of risk, and address common frustrations related to disaggregation of data.

Source: ADB

143. While it is up to the jurisdiction to decide how best to bolster understanding of TBML risks, jurisdictions should ensure that measures aimed at expanding public and private sector knowledge of TBML are commensurate to the level of risk.

6.2. Financial intelligence collected by FIUs

144. As the central hubs for financial intelligence within their countries, FIUs have a number of valuable sources of information that can help uncover potential TBML cases. By combining data from these different sources, FIUs are in a unique position to detect and analyse possible TBML schemes and then disseminate the appropriate financial intelligence to their national and international partners. Because the analysis by FIUs frequently serves as the trigger for further public action, it is crucially important that FIUs have a well-developed understanding of TBML and sufficient resources to produce the respective financial intelligence. While the sources of information used by FIUs in TBML cases, and the analysis carried out, may be similar to those used for other ML/TF cases, they also have some TBML-specific aspects, as described below.

145. The foundation of FIU data is the suspicious transaction reporting that FIs and DNFBPs are obliged to submit when they detect suspicious activity by their clients. Because STRs are often the starting point of the FIU's analysis in ML/TF cases generally, the quality and accuracy of the information contained in these reports have a direct impact on the quality and timeliness of the FIU's analysis. For TBML cases, which has both trade and financial transaction components, this is equally relevant. For example, an STR providing not only a description of the suspicious financial transaction(s) – with details on the involved parties and the basis of suspicion – but also insights into the corresponding trade activity and related information, may boost the FIU analysis.

146. FIs are in a unique position to provide valuable leads to FIUs for detecting possible TBML schemes, given their involvement in trade finance, their knowledge of customer behaviour, and their role as a financial intermediary, executing payments on behalf of the customer. With respect to trade finance specifically, FIs often have direct access to documentation underlying the trade transactions. In addition, FIs may have an incentive to carry out enhanced due diligence on the customer when extending funding for the customer or providing guarantees of the client's financial status and stability. With respect to open account trade and correspondent banking, FIs may generally have less information about the client and its activities, but they can nonetheless identify suspicious activity through the detection of anomalies, such as transactions that differ from normal customer behaviour and other unusual transaction patterns.

Infographic 6.1. Categories of reports submitted by FIs to FIUs

Reports relating to trade finance

The FI is directly involved and has access to underlying documents related to the trade transaction, through which it detects e.g. irregularities in the documents and/or in the customer's / counterparty's activities or in the information provided during the trade finance process.

Reports on open account settlements of trade transactions of a customer

Underlying documents are not generally available to the FI, however, the FI detects e.g. irregularities in the customer's financial activities related to trade and / or in their transactions and / or irregularities connected to their counterparties.

Reports on trade transactions in correspondent banking

The FI has no access to underlying documents or customer information, however, it detects e.g. irregularities on cross-border transactions, including those allegedly for goods and trade, and / or identifies suspicious parties potentially related to previously identified ML networks or ML activities.

Source: Egmont IEWG

147. STRs submitted by DNFBPs, especially notaries, auditors, and accountants, can be another source of valuable information for FIUs about possible TBML schemes. Based on their professional experience and AML/CFT knowledge, these professions are well-positioned to identify and recognize companies that are used solely to hide the original form of the payment and other complex legal structures established for money laundering activities. STRs focusing on such corporate structures can be of significant value for detecting TBML, since front and shell companies have been identified in a wide range of TBML techniques.

148. In addition to STRs submitted by DNFBPs and FIs – as required by the FATF Recommendations – some FIUs receive STRs from other sectors, such as commercial entities engaging in international trade. This reporting can be a useful tool for detecting TBML, especially if such reporting comes from sectors particularly vulnerable to TBML. Although an increased reporting from these entities bears the potential to substantially contribute to the detection of TBML, such measures could not substitute the insufficient level of reporting from DNFBPs noted by FIUs in some jurisdictions.

Box 6.7. Example of other sectors been designated as reporting entities

Under the national legal framework, "traders of goods" (including industrial producers such as car manufacturers, etc.) are designated as reporting entities in Germany. Germany's FIU thus receives STRs from such companies, including reporting on suspicious amounts being paid into their customers' accounts by unknown third parties. Such reporting has allowed the German FIU to detect some potential cases of TBML.

In one such case, a car manufacturer reported to the FIU that a number of payments on behalf of sales partner A located in country X were made from various third-party accounts at banks in different countries. The third-party payers, which were registered in various jurisdictions, were all unknown to the car manufacturer. Analysis of incoming payments from the past years revealed that funds transferred by various third-party payers on behalf of A amounted to over € 50 million.

A second car manufacturer identified and reported third-party payments for sales partner B located in the same country X. Analysis revealed that the two sales partners, A and B, actually shared the same ultimate BO, a national of Country X. Third-party payments on behalf of B amounted to over EUR 30 million. One of the third-party entities involved had been noted as a "core company" of one of the so-called "laundromats".

Source: Germany/Egmont IEWG

149. Given the cross-border nature of international trade, real-time information exchanges between FIUs are also critical to the detection of TBML. By reaching out to their direct counterparts in over 160 countries, FIUs can obtain additional administrative, law enforcement, and financial information on natural and legal persons, as well as transactions involved in specific cases. Data received from foreign FIUs can help identify a TBML component of an already existing case or prompt a new FIU analysis that uncovers new TBML schemes.

150. The significance of international cooperation and information exchange was underscored by a number of cases provided. A number of FIUs noted that information gathering and subsequent analysis on some TBML schemes were possible only because of feedback from their counterparties in other jurisdictions. In addition, the timely exchange of information and cross-border support, such as postponement of transactions based on a foreign request and forming taskforce teams of experts from the relevant jurisdictions to work on common cases proved essential for investigations and asset recovery in a number of cases. Close cooperation and the exchange of data between FIUs at the international level, both bilaterally and multilaterally, are thus an essential component of combatting TBML. Diagonal cooperation through the relevant foreign FIU with its domestic LEAs, customs or other competent authorities has also proven to be an effective mechanism for intelligence collection and verification of the initial suspicion.

6.3. FIU analytical approaches to TBML

151. FIUs play a central role not only in processing STRs but also in producing more sophisticated analysis on TBML schemes. In carrying out their analyses of data and information received from different sources – including reporting entities, administrative and law enforcement authorities, and international counterparts - FIUs combine the relevant

pieces of intelligence to frame a more complete picture of the financial scheme, which can enable the detection, substantiation, or possible negation of a TBML case. Analyses conducted by FIUs on TBML cases can include, for example, the comparison of information on flows of goods and flows of funds, to initially identify anomalies or to sustain questionable variances and reports on suspicious trade related transactions.

152. While this "classic" operational analysis, relying on comparisons between trade and financial data to detect possible anomalies, seems to be the most common way for FIUs to identify TBML cases, some FIUs also have experience in identifying possible TBML schemes by approaching this issue from another angle. This approach involves the analysis of corporate structures, registration details, alleged company purposes, corporate banking profiles, and the relationship between corporate networks, such as common representatives, overlapping ownership structures, identical registration addresses, and joint bank accounts. By determining with some certainty that an "international trading corporation" was nothing more than a complex set of shell companies, FIUs may be able to assume that the various trade transactions conducted between these "subsidiaries" are fictitious. Based on these initial findings, authorities can launch an investigation into the TBML scheme. This "reverse" approach underscores the importance of collecting and joining different pieces of financial intelligence and other available data, and shows that the analysis and detection of TBML does not necessarily require supporting trade documentation in all instances.

153. Venturing further into new avenues of analysis and discovery, FIUs have highlighted the importance of building the capacity to process large data sets, including through the use of analytics and visualization tools. They also emphasize the increasingly critical role played by matching technology (i.e., thematic match filter) in their analytical work. Because trade-related transactions are often complex and multijurisdictional, innovative IT solutions, such as graph analytics and artificial intelligence (AI) and machine learning, can be particularly helpful in TBML-related analysis conducted by FIUs. Such solutions can be used not only to analyse large data sets, but also to fill in missing links in existing networks (for example, identifying unknown criminal networks based on known criminal networks) and pinpointing interactions that indicate fictitious trade activities.

154. Strategic analysis is one of the core functions of any FIU. In practice, FIUs use different approaches to perform this function, depending on the available resources and the structure of the domestic AML/CFT framework. But ultimately, the FIU's strategic analysis should lead to an increased understanding of the risk for the FIU, other authorities, financial institutions, and the public at large. For TBML-related cases specifically, FIUs can provide these groups with insight into the potential size, scale, and most commonly used methods, thus contributing to an improved understanding of the risks.

Box 6.8. Strategic analysis conducted by the Italian FIU

The Italian FIU, in collaboration with the Statistical Analysis Directorate of the Bank of Italy, has developed an empirical analysis of the bilateral statistics on Italy's foreign trade.[24] The analysis is based on the evaluation of discrepancies between statistics held by Italy and partner countries on goods traded over a period of four years.

The value of imported or exported goods recorded in one country rarely coincides with the corresponding value of exported or imported goods registered in the trade partner country, also known as mirror statistics. A number of objective factors can cause this misalignment, including insurance and freight costs, cultural and language difference between the countries, inefficient reporting systems, and differences in goods classification criteria, as well as deliberate misreporting.

By following a well-established strand of economic literature on international illegal financial flows, the analytical methodology implemented by the Italian authorities allows to control for the main 'legal' sources of mirror statistics discrepancies and identify, with a reasonable degree of approximation, purposeful false declarations associated with illicit cross-border transfer of funds. The final objective is to identify anomalous trade flows and accordingly define TBML risk quantitative indicators related to countries and products at sector level.

Based on the operational analysis carried out by the Italian FIU and exchanges of information with other national authorities, some of the findings have been linked to potentially illicit transactions.

Other countries could replicate this approach, since the relevant data used in the study is produced by international organisations (United Nations Conference on Trade and Development, World Bank and Organisation for Economic Co-operation and Development) for all countries.

Source: Italy

155. Despite this potential to detect ML, in many jurisdictions FIs and DNFBPs still experience challenges with identifying TBML (see Section 5.5), that often results in low quality STRs or a lack of reporting. In this regard, jurisdictions should take steps to ensure that their FIs and DNFBPs have the necessary capabilities to identify suspicious transactions and promptly report them to the FIU. Such steps may include communicating NRA findings to FIs and DNFBPs, including how criminals have been misusing or may misuse a particular sector for TBML schemes. Other steps may involve targeted trainings and the provision of risk indicators and feedback from the FIU that may support FIs and DNFBPs in their efforts to identify TBML. Generally, the more concrete and detailed information on TBML FIs and DNFBPs would get from the public sector, opposed to generic and vague descriptions of the risk, the more positive impact these steps may bring. These measures should also be coordinated with the respective supervisory authorities.

[24] Gara, M., Giammatteo, M., and Tosti, E. (2019), 'Magic mirror in my hand… How trade mirror statistics can help us to detect illegal financial flows', *The World Economy*, 42: 3120--47.

6.4. Role of customs in countering TBML

156. Custom services are usually the primary enforcement authorities in the trade area, with a mandate to tackle crimes based on the misuse of the international trade system, including TBML. Customs services thus have in-depth knowledge of the international trade arena, the flows of goods, and international supply chains, all of which are vital for identifying and investigating TBML activities. Customs services also often have sole access to international trade documents and data, which is key to identifying TBML. Custom cargo analysis, in particular, can be used to detect TBML, as anomalies in this data can indicate a TBML scheme and other trade-related crimes.

157. The role of customs services as the sentinels for illicit trade activity places these authorities in a unique position for detecting the use of international shipments for illicit purposes. At the same time, the ever-increasing volume of international trade – and the associated increase in trade data – presents a key challenge for customs services trying to identify TBML schemes and other trade-based crimes. Shipments associated with TBML represent a small fraction of the overall legitimate trade, making TBML challenging to identify. In addition, customs services must balance the analysis and inspection of cargo shipments with the need to clear shipments quickly and ensuring a viable and efficient trade framework. Other historical priorities of custom services, such as the collection of custom duties and setting tariffs, also require significant resources. Therefore, it is important to ensure that custom services have sufficient capacity to examine shipping documentation and financial intelligence provided by the domestic FIU and LEAs[25]. This, for example, can be addressed by establishing dedicated units or divisions with custom services to focus on this area and thus ensure that counter-TBML efforts are maximized.

158. During their day-to-day activities, customs services regularly encounter many of the AML methods used by organised criminal groups for laundering illegal proceeds, especially those involved in the placement and layering stages. In the case of TBML specifically, money can be laundered through the international movement of commercial assets, which are normally traded or shipped for purposes of commercial profit. These assets can include a wide range of commodities, such as electronics, raw materials, clothing, jewellery, and food stuffs, as discussed above. In this sense, customs officers have an essential role in analysing and identifying goods and shipments that could be used in TBML networks.

159. Close collaboration between customs agencies and FIUs greatly enhances the collective capacity to identify TBML by linking suspicious trade activity with suspicious financial activities. In TBML cases, the investigation of predicate offences at the domestic level is often linked to investigations of international money laundering, as LEAs follow the trail of money and goods into the customs arena. This is especially true for cash-intensive criminal activities in which OCGs convert the illicit funds into commercial products for international shipment. Thus, it is particularly important that custom authorities, the FIU, and LEAs synchronise their efforts in the AML/CFT area, especially in countries with elevated TBML risk.

[25] In some jurisdictions, customs and LEAs may have direct access to financial intelligence developed by FIUs.

Box 6.9. Customs-FIU cooperation in Peru

The FIU of Peru provides in-house internships for Peruvian customs authority officials. This allows, for example, for an official specialized in customs operations to develop his/her skills while working as an intern at the FIU, developing knowledge on financial analysis, and preparing financial intelligence reports that will be ultimately sent to his/her agency. Using this approach allows the expert to understand how both agencies work.

Source: FIU-Peru

160. This collaboration should include swift information sharing between the abovementioned authorities, and coordination of the investigative and operational responses to TBML and related predicate offences (see section on interagency working groups below). While the form this collaboration takes is often heavily dependent on the structure of the domestic legal framework (e.g., which authorities have the mandate to investigate TBML and cash smuggling; whether customs authorities have investigative powers; and whether they can investigate ML), there are certain best practices that apply to most domestic law enforcement frameworks.

161. The WCO/Egmont Group's Customs-FIU Cooperation Handbook recommends that customs services and FIUs establish robust partnerships at the national level. These partnerships should be formed at the senior management, front-line manager or officer, and analyst levels. The handbook specifically encourages quarterly or twice-yearly mid-level management meetings, so that strategic plans can be put in place to combat TBML and suspicious financial information can be exchanged for both intelligence and operational purposes. Where allowed by domestic legislation and agency policies, such collaboration may also include the sharing of trade and financial data, including information on individuals and legal entities suspected of conducting customs-centric money laundering activities, customs fraud, or smuggling activities. Many such cases of illicit activities include TBML activity.

Box 6.10. German customs – FIU cooperation

The Auditing Service of the German Customs Service has an information sheet on the involvement of the Auditing Service in the fight against money laundering and terrorist financing, as well as an associated typology paper.

When foreign trade audits, customs audits, fiscal audits, market organisation audits, and tax audits reveal evidence of ML, the information sheet describes the next steps the auditor and Auditing Service should take. In particular, the Auditing Service is asked to send the suspicion of ML directly to the FIU using the goAML web application.

Source: Germany

162. The FIU's financial analysis expertise and customs services' international trade expertise, coupled with effective information sharing mechanisms between the two authorities, can lead not only to increased efficiency of AML/CFT measures, but also contribute to other customs services objectives. For example, gathering information about

high-risk sectors and patterns of TBML activity, as well as using the outcomes of FIU strategic analysis and other strategic information related to international trade shipments, may help customs services improve their prioritization of cargo and shipment inspections. Introducing advanced analytical techniques within custom services may also help to increase the identification of trade-fraud activity and other trade related crimes. It may also assist customs in establishing "hot routes" and new schemes utilised by criminals and terrorists.

163. It is also important for customs services to recognize counter-TBML efforts as a priority enforcement objective and collaborate with each other on bilateral and multilateral bases. TBML schemes often generate a large volume of supporting documentation. Portions of this documentation are intended for passing mandatory clearance of the shipments from one customs jurisdiction to another. This customs documentation is also used to justify the transfer of payment for the goods that are shipped. The customs documentation in the importing jurisdiction can vary from the documentation presented in the exporting jurisdiction, as criminals often falsify this documentation to earn illicit profits or to move illicit value. Thus, the comparison of inbound and outbound shipping documentation conducted by the respective customs services may lead to the detection of trade anomalies, some of which could be part of a TBML scheme.

Box 6.11. CBSA: Trade Fraud & TBML Centre of Expertise

In recognition of the threat posed by TBML in Canada, and the critical role played by the Canada Border Services Agency (CBSA), Canada's customs service, in addressing the issue, Canada authorized the creation of the Trade Fraud and Trade-Based Money Laundering Centre of Expertise within the CBSA. The Centre was operational as of April 2020 and is mandated to enhance the CBSA's capacity to identify, interdict, and investigate complex trade fraud and to refer TBML files to the Royal Canadian Mountain Police. By establishing a multi-disciplinary team comprised of intelligence analysts, trade specialists, and criminal investigators, the CBSA is better positioned to identify and investigate anomalous trade transactions indicative of TBML, and fill in knowledge gaps on threat actors and "modi operandi".

Source: Canada

6.5. Interagency groups and coordination bodies

164. Cooperation and coordination among competent authorities is a key factor in the successful detection and disruption of any ML and TF activities. For TBML, effective collaboration between law enforcement, prosecutors, FIUs, customs services, and other authorities, as well as swift information-sharing mechanisms, is even more crucial, due to the complexity and variety of actual TBML schemes. For TBTF, having effective cooperation and information sharing with intelligence agencies is also necessary given the inherent nexus of TF related intelligence to the detection of TBTF schemes. Although this report does not aim to set forth a required framework and there is no "silver-bullet" solution in the context of TBML, jurisdictions may want to take into account some of the factors below when establishing a new interagency group to pursue TBML or expanding the mandate of an existing group.

165. The multi-dimensional nature of TBML gives authorities additional opportunities to detect ML. As identified above, criminals combine TBML techniques with other laundering methods, like the use of front companies and frontmen or transmitting funds via

complicit FIs. Thus, identifying one element of the ML scheme may lead to the discovery of the whole scheme. Depending on the misused sector and particular technique applied by criminals, different authorities may be better placed to detect TBML. At the same time, identifying TBML schemes in full and tracing criminal proceeds requires mapping multiple pieces of financial and trade information which is only possible if the relevant authorities provide assistance to each other. In order to do so efficiently, authorities need to have mechanisms in place allowing them to communicate their knowledge and expertise of TBML to LEAs in a timely manner and vice-versa. Given that a TBML investigation can involve multiple agencies, establishing a coordination mechanism or a working group – whether under the umbrella of one agency or as a separate platform – can lead to increased efficiency.

166. While jurisdictions may opt to use a variety of models in structuring such collaboration, such as a working group or "fusion centre" exclusively focused on TBML or treating TBML as part of a broader ML mechanism, it is important to ensure that TBML is recognised as a priority proportionate to the risk it poses to the national financial and trade systems. Such prioritisation should serve as a safeguard, allowing authorities to assign and efficiently use their expertise and resource, either on trade or financial or other aspects of TBML.

167. As with any other consensual crime, identifying TBML can pose particular challenges, as there will likely be no victim making complaints to authorities. Authorities often have to rely on other means to detect TBML, some of which require the comparison of large volumes of data. In addition, some PML networks using TBML schemes to move funds across borders may rely on myriad transactions and trade operations, and numerous frontmen and shell companies, whose only purpose may be to disguise the illicit nature of the transferred funds and confuse the authorities. Thus, establishing a mechanism allowing cross-comparison and matching of large volumes of data in a timely manner is important not only for the detection of TBML, but also for the identification and tracing of assets. Regardless of where the mechanism is placed, whether within one agency or under the umbrella of an interagency group, its creators should ensure that it can count on a wide range of information sources, such as STRs, trade data, basic and beneficial ownership information, criminal records, and registries of property (land, cars, etc.).

Box 6.12. National Cargo Diagnostic Centre

In 2014, Israel established the National Cargo Diagnostic Centre to monitor international trade operations, focusing on goods that may be exploited by terrorists. The centre is located in the Israeli Tax Authority and includes representatives from other LEAs and security agencies. The centre uses a dedicated risk assessment IT system to identify trade activity that is used to smuggle terror-related goods and goods used for terrorism financing. If suspicious transactions related to ML are detected, information is sent to the relevant investigative unit(s) for further investigation.

Source: Israel

6.6. Public-private partnerships

168. PPPs are a way for public authorities and a selected group of private sector entities to collaborate and efficiently achieve mutual goals. In the AML/CFT context, PPPs are usually seen as a platform to share information and knowledge about existing ML/TF

typologies, identify new and emerging risks, and exchange information. In some jurisdictions, PPPs also serve as an additional channel of exchanging financial intelligence between operational authorities and reporting entities.

169. The FATF Recommendations contemplate cooperation between the public and private sector on AML/CFT matters[26], but they do not explicitly require jurisdictions to establish a PPP to meet this requirement. At the same time, PPPs may be a useful way to increase communication between the involved sectors and even contribute to a broader dialogue. For TBML schemes, such communication may be even more critical, since countering this form of ML requires significant expertise from both authorities and the private sector.

170. Jurisdictions that seek to create a PPP in the AML/CFT field or enhance the effectiveness of an existing partnership may opt for different models, taking into account the risks and other features of the domestic AML/CFT regime. While some jurisdictions have chosen to establish a PPP specifically targeting TBML as the main objective, others preferred to apply a PPP model in which TBML is treated one among many ML issues. Regardless of the model chosen, jurisdictions may want to take into account the following:

- While some PPPs may have an informal structure, without formal rules or procedures governing their activities, it is important to reach a clear agreement among the participants on the objectives of such collaboration and the division of roles. This agreement should serve as a basis to establish trusted relationships between the public and private sector.
- Setting up a PPP should not be seen as the goal per se, but rather as a tool to address a particular area of concern in the national AML/CFT regime or to increase the effectiveness of domestic AML/CFT measures. One way to ensure this is to identify short- and long-term goals before establishing the PPP. In the context of TBML, these goals could include increasing understanding of vulnerabilities of the trade and financial systems and improving information sharing.
- Depending on the objectives and priorities of a PPP, the numbers of participants, and their level and sectors or authorities, may vary. If TBML is among the PPP's priorities, it is important to ensure that the PPP has the relevant expertise, including trade, customs, and trade finance.
- While the concept of a PPP implies the direct involvement of a limited number of private sector participants, this does not mean that the outcomes of such collaboration – such as guidance documents and red flags indicators –would not be useful for a broader audience. Jurisdictions may consider communicating the achieved outcomes, particularly related to risk identification and assessment, to the private sector entities that are not directly involved in the PPP to improve understanding of TBML risks across the sector or sectors.
- When a PPP involves the exchange of information at the operational level, such as the sharing of information traceable to subjects (personally identifiable information, financial transactions, etc.), authorities should make sure that such exchanges comply with the domestic data privacy and other relevant laws and regulations.

[26] For example, competent authorities should provide guidance and feedback to FIs and DNFBPs in applying AML/CFT measures.

171. The below boxes provide an overview of different types of PPPs focused on AML/CFT issues, including related to TBML.

Box 6.13. German PPP and cooperation with the private sector

In September 2019, Anti Financial Crime Alliance (AFCA), a public private partnership was established in Germany. AFCA is a response to the risks identified in the German NRA. The main objective of AFCA is to improve cooperation in the fight against money laundering and terrorist financing in Germany between the public and private sector. The PPP consists of representatives of the Federal Criminal Police Office, Federal Financial Supervisory Authority and the Financial Intelligence Unit as well as 14 representatives of the private banking sector. At its meeting in December 2019, AFCA decided to create a private sector led task force focusing on TBML.

To advance the fight against money laundering in a targeted, public, and effective manner, Germany carried out the first national "Concerted Action against Money Laundering" at the end of November 2019, with the participation of its FIU and supervisory authorities for the trade in goods. The action was focused on the auto parts and vehicles sector.

The FIU has also carried out two symposia with supervisory authorities of DNFBPs. Furthermore, the FIU has participated in several meetings of the supervisory authorities for trade in goods. These activities were intended to explain the FIU's activities and to initiate and increase cooperation. Further cooperation of this kind is planned.

Source: Germany

Box 6.14. Fintel Alliance TBML Working Group

In early 2020, Australia's PPP, Fintel Alliance, established a dedicated TBML working group aimed at building resilience, sharing knowledge, and developing coherent strategies to combat and disrupt TBML in Australia. The working group, which meets on a monthly basis, comprises subject matter experts from government, law enforcement, and financial industry partners.

One of the objectives of the working group is to identify and document how financial facilities and products are exploited for TBML purposes. The working group also aims to consider and review the adequacy of the controls to mitigate TBML. The working group will cultivate domestic and international partnerships, and develop typologies and indicators to establish best practices that enable an enhanced and collaborative response to combating TBML. In the short period of time since its establishment, the working group has launched a number of initiatives, including:

- The development of a TBML indicators paper comprising feedback from public and private partners.
- The establishment of an information-sharing framework for public and private collaboration under the guidance of the Australian Border Force, for the purposes of identifying and reporting suspicious activities in selected high-risk industry sectors.

- The creation and delivery of a dedicated training program on trade financing by a financial institution.

Source: Australia

Box 6.15. PPP focused on cash integration

Since 2018, the Anti Money Laundering Centre (AMLC) has been inviting relevant public and private organisations to further develop their knowledge and understanding of TBML.

In 2020, these sessions evolved into a structural collaboration under the flag of the Financial Expertise Centre (FEC). As part of this collaboration, both public and private parties work together in combatting the cash integration variant of TBML in the automotive sector. The PPP involves various stakeholders, including the FIOD, the four biggest Dutch banks, the FIU, the National Police, the prosecutor's office, and tax authorities.

This collaboration is focused on combating various forms of illicit cash integration in the automotive sector. Besides knowing your customer, it is important to know your sector (KYS) and the automotive sector in the Netherlands is perceived as being cash based. However, the initial results of the PPP's work show the sector isn't as cash based as thought. There are only several companies accepting large amounts of cash, with payments in cash being only sporadic rather than regular.

Bringing together leading public and private sector experts, the Dutch PPP is developing proposals for enhancing the sector's regulation, for example arguments for business to business cash payments. The PPP is also producing typologies and indicators of TBML activity tailored to the sector, which should assist authorities in detecting rogue car sellers and buyers, as well as strengthen their understanding of the whole sector.

Source: the Netherlands