FATF • GAFI
Financial Action Task Force Groupe d'action financière

FATF Report

Global Money Laundering & Terrorist Financing **Threat Assessment**

A view of how and why criminals and terrorists abuse finances, the effect of this abuse and the steps to mitigate these threats.

July 2010

THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

WWW.FATF-GAFI.ORG

FOREWORD

I have pleasure in publishing the first Financial Action Task Force (FATF) Global Money Laundering and Terrorist Financing Threat Assessment (GTA). This document presents a global overview of the systemic money laundering (ML) and terrorist financing (TF) threats and ultimate harms that they can cause.

Since 1989, the FATF has led efforts to adopt and implement measures designed to counter the abuse of the international financial system by criminals. The FATF established these measures or "Recommendations" in 1990 and has revised them periodically so that they remain up to date and relevant to the evolving threats posed by money launderers and terrorist financiers. The measures set out the basic framework for anti-money laundering and countering the financing of terrorism (AML/CFT) efforts. In developing the measures, the FATF has examined ML/TF techniques and trends through typologies studies to identify current and emerging threats to the financial system.

The FATF has published over 20 typologies reports examining various thematic and sectoral areas vulnerable to ML/TF. This work is ongoing because typologies need to be re-assessed to reflect changes in the financial and trade systems that criminals and terrorists may take advantage of, as well as the evolution of the techniques they may develop over time to subvert control mechanisms. The FATF has recently intensified its surveillance of the systemic ML/TF threats to enhance its ability to identify, prioritise and act on these threats. The GTA represents new thinking about these threats.

The GTA provides a view of the most prevalent ML/TF threats which have been identified over the years as causing harm. Much of this information has been derived from studies of ML/TF techniques and methods conducted by the FATF, FATF-Style Regional Bodies (FSRBs) and by jurisdictions themselves. By laying out the information in this way, the GTA also provides a framework that can be used by jurisdictions for tackling these threats.

This document has been produced by a diverse project team comprising members from law enforcement and other agencies responsible for identifying and combating ML/TF from many jurisdictions. It therefore represents an endeavour never attempted before globally.

There are over 180 countries throughout the world which are engaged with the FATF in taking action to minimise the threats of ML/TF. Over the years, much has been done by governments and intergovernmental, multi-lateral organisations, the private sector and academics to understand what it takes to make it more difficult for money launderers and financiers of terrorism to operate. However, the problem of ML/TF remains and requires ongoing efforts. Notably, greater efforts should be given to implementing measures aimed at detecting and taking enforcement actions against individuals and organisations who conduct these serious illegal activities.

I hope that this assessment will raise the level of understanding of the threats that ML/TF can pose and the negative impact that result, and help governments to take decisive action to minimise those harms. More importantly, I hope it will provide information to governments, the private sector and international policy-makers that will help to better manage scarce resources and take more focused action against ML/TF.

Paul Vlaanderen
FATF President, 2009-2010

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

1. This chapter starts by describing the role of the Financial Action Task Force (FATF) in the effort to combat money laundering (ML) and terrorist financing (TF). It then describes the FATF's Strategic Surveillance Initiative and the main findings contained therein. The next sections of the chapter explain what the Global Money Laundering and Terrorist Financing Threat Assessment (GTA) aims to achieve, describe its framework and then lay out how that framework can be used as a tool by governments. Next the chapter goes on to describe the overall harms of crime and terrorism. The following section discusses the global financial crisis. The final two sections of the chapter contain some key terms and describe the information sources used for the GTA.

1.1. The FATF on Money Laundering and Terrorist Financing

2. The priority of the FATF is to ensure that global action is undertaken to combat ML and TF. In recognising the threat posed to the financial system and to financial institutions, the FATF has been at the forefront of measures to counter attempts to abuse the financial system to further criminal and terrorist purposes.

3. Since its creation, the FATF has taken concerted action to combat this threat by focusing its work on three main activities:

- *Setting global standards to combat ML/TF:* in order to increase the transparency of the financial system (making it easier to detect criminal activity) and give countries the capacity to successfully take action against money launderers and terrorist financiers.

- *Ensuring effective compliance with the standards:* through the mutual evaluation process to monitor the implementation of the 40+9 Recommendations in its member jurisdictions and assess the overall effectiveness of anti-money laundering (AML) and counter financing of terrorism (CFT) systems.

- *Identifying ML/TF methods and trends:* through typologies studies to inform regulatory authorities, law enforcement, the financial sector and the general public about specific ML/TF threats and provide the necessary basis for informed national and global policy-making on how best to address these threats.

4. To date, over 180 jurisdictions have joined the FATF or an FATF-Style Regional Body (FSRB), and committed at the ministerial level to implementing the FATF standards and having their AML/CFT systems assessed.

5. Going forward, the FATF will continue building on this work to protect the integrity of the international financial system and to respond to new and emerging ML/TF threats.

1.2. The Strategic Surveillance Initiative

6. As part of its current mandate[1], the FATF aims to deepen the global surveillance of evolving criminal and terrorist threats. The FATF has therefore determined that it must be more active in identifying systemic criminal and terrorist threats involving the international financial system. This enhancement to the typologies process will then intensify the FATF's ability to identify, prioritise and act on these threats.

7. To meet this need, a new mechanism – the "Strategic Surveillance Initiative" – was established in 2008. The objectives of the Strategic Surveillance Initiative are to: (1) detect and share information on the types of criminal or terrorist activities that pose an emerging threat to the financial system, and (2) develop a more strategic and longer-term view of these threats. This initiative involves the use of a detailed questionnaire which both FATF and FSRB members respond to on a yearly basis. Jurisdictions are asked to provide information on the ML/TF methods, techniques and trends they are experiencing as well as to identify the sources of ML and terrorist finance.

Summary of main sources of money laundering

8. The 2009 FATF Strategic Surveillance Survey showed that illicit funds laundered through the financial system come from a variety of sources. All 20 designated categories of offences in the glossary of the FATF Recommendations have been identified as sources of criminal proceeds. Responses to the 2009 survey from numerous jurisdictions identified white collar crimes (tax, fraud, corporate crimes, embezzlement and intellectual property crimes) and drug related crimes as the major sources of criminal proceeds.[2] For example, a significant number of jurisdictions noted that they have increasingly seen internet-based frauds and other use of internet technologies in fraudulent predicate activities.[3]

9. The smuggling of goods and contraband has also been identified as another main source of illicit proceeds. Also, taxation or excise evasion, while currently not specifically classified as a designated category in the FATF glossary, has been identified as a major source of illicit funds. Corruption and bribery (including the embezzlement of public funds) have also been highlighted.

Summary of main sources for terrorist financing

10. Similar to criminal networks, terrorist organisations also derive funding from a variety of criminal activities ranging in scale and sophistication from low-level crime to involvement in serious organised crime. The 2009 survey showed financial crime (particularly fraud), trafficking in narcotics, cigarettes, weapons, human beings or diamonds and petty crime being the most commonly identified sources.[4] Furthermore, terrorist organisations raise funds through legitimate and illicit activities but more

---

1 On 27 February 2008 the FATF revised its mandate for 2008-2012 to ensure that it is able to respond with flexibility to new challenges. See *www.fatf-gafi.org*.

2 Presentations by Belgium, Japan and Singapore to the FATF Working Group on Typologies in February 2009 gave case details of money laundering related to fraud and other white collar crime and the involvement of professional advisors to facilitate these crimes.

3 Consistent with this, numerous mutual evaluation reports have shown that the most important sources of criminal proceeds laundered are narcotics trafficking and various fraud schemes.

4 Consistent with this, a number of mutual evaluation reports showed narcotics trafficking to be the most prevalent criminal activity used to raise terrorist funds. This is followed by fraud, then smuggling and extortion.

commonly through a mixture of both. The 2009 survey reported fund raising/donation, charities and non-profit organisations (NPOs) and small cash-intensive businesses as the most prevalent legitimate sources[5].

Identifiable global trends

11. Both the 2008 and 2009 strategic surveillance exercises showed that the ML/TF methods and techniques that most jurisdictions are currently seeing are broadly the same as the ones that have been observed and described in previous FATF exercises. In line with 2008, the 2009 exercise highlighted that a noteworthy proportion of ML/TF activity involves cash. Cash couriers and cash smuggling continue to be used, and cash placement is still an important activity for money launderers and terrorist financiers.

12. Some emerging issues have been detected however. In relation to ML, the 2009 survey showed an increased use of internet-based systems and new payment methods. The abuse of new forms of payment methods has been reported (although the adoption of such new or emerging technology by criminals can be seen as increasing in line with the trends in society as a whole). The surveillance exercise also showed that some jurisdictions have seen new or increasing use of complicated commercial structures and trusts for ML.[6]

13. Where new activity or increasing methods are observed, it is not always necessarily because the activity is new or occurring at a higher rate, rather it may be that the activity is being detected more effectively. For example, some jurisdictions have reported an increasing use of cash. However, the techniques associated with cash are already familiar in other regions, and represent a significant volume of ML activity.

14. Finally, the 2008 and 2009 surveys noted the primary techniques identified for moving terrorist funds were the physical movement of cash (*e.g.*, cash couriers), wire transfers involving cash deposits and withdrawals, and alternative remittance systems. While most jurisdictions were not able to identify any new trends in moving terrorist funds in 2009, a wide range of new techniques were identified from the remaining respondents. A number of new techniques and methods observed, while not necessarily indicating a trend, included the following: use of new payment methods, involvement of transactions related to the purchase and export of cars, involvement of a property holding company to collect funds and disguise their final destination, a link with trafficking in weapons and trade-based activities.

Overview of systemic criminal and terrorist threats

15. A number of global systemic threats have emerged based on FATF's work described above. Three particular issues stand out. First the significance of financial crimes, and in particular fraud, cannot be understated. Fraud activity – including various types of internet fraud and tax fraud – appear to represent the primary source of proceeds of crime found to be laundered and this appears to be an increasing trend. Second, despite criminals' maximising the opportunities present in new technologies, new financial products and new commercial activities, the abuse of cash remains of concern. Use of cash couriers and bulk cash smuggling continues. Lastly, it should be recognised that ML and TF activities are predominantly global in nature, often involving more than two jurisdictions, with rapid movements and investment of proceeds of crime.

---

5 Consistent with this, the use of charities and NPOs continues to be the leading source of funds as reported in Mutual Evaluation Reports.

6 For example, complicated commercial structures and trusts involving the use of off-shore entities and front companies, the involvement of professional advisers, complicit bankers, use of fictitious loans and trade based money laundering (TBML) and the co-mingling of licit and illicit funds.

1.3. FATF Global Money Laundering and Terrorist Financing Threat Assessment (GTA)

16. The *FATF Global Money Laundering and Terrorist Financing Threat Assessment (the GTA)* is based on the in-depth typologies studies and the Strategic Surveillance Initiative noted above. It is designed to provide a strategic and long-term view of ML/TF threats.

17. The GTA takes the approach established by FATF and builds on it using its own framework to provide an overview of systemic ML/TF threats, including new thinking about why they exist and what harms they cause. This assessment presents a different way of thinking about ML/TF threats:

- Rather than examining the wide array of ML/TF techniques, the GTA offers a simplified approach by recognising that most ML/TF activity must utilise at least one of five features.

- The GTA provides an understanding of *why* criminals and terrorists conduct their finances using those features and considers what factors exist to allow for successful ML/TF. This allows for new thinking about how to control use of those features to create a more hostile environment for criminals and terrorists to operate in.

- The GTA recognises the impact and effect of successful ML/TF on the international financial system but goes beyond this to include the impact and effect of this activity on individuals, on non-financial businesses, on local communities and on national and international interests. These are described in terms of the 'real world' outcomes of successful ML/TF – *i.e.* the resulting harms. This extra dimension allows readers to consider countering the ultimate aims of money launderers and terrorist financiers, thereby indirectly reducing the threat to the financial system.

18. The GTA does not attempt to quantify the value and volume of ML/TF activity due to the lack of reliable and consistent statistics at a global level. In carrying out the research for this project, it became apparent that these statistics were not necessary to be able to recognise the components of ML/TF, the harms caused and the need for global action.

19. There is no one-size-fits-all way of understanding and means of devising responses to ML/TF threats. Thus, the GTA uses a tailor-made framework. While designed specifically to underpin the analysis in the GTA, that is, at the global level, the framework is equally relevant to national level assessments and strategies. Indeed, it is one of the aims of this report that the framework be made available for use by governments in developing and conducting national assessments, while taking into account their own particular circumstances, in order to better understand the ML/TF threats their countries face.

1.4. The GTA Framework

20. The GTA framework sets out:

- The *features* that are abused by money launderers and terrorist financiers. These features are the building blocks of ML/TF as almost all ML/TF activity must utilise one or more of these features. As such, the body of this report comprises of five distinct sections, each focusing on a particular feature of ML/TF, covering in turn:

  - Cash and Bearer Negotiable Instruments (Chapter 2).

  - Transfer of Value (Chapter 3).

  - Assets and Stores of Value (Chapter 4).

- Gatekeepers (Chapter 5).
- Jurisdictional/Environmental Aspects (Chapter 6).

- The main *harms* that are caused by the abuse of these features.
- The *drivers* and *enablers* (or reasons for use) that attract criminals and terrorists to these features and allow them to be abused.
- How the harms can be reduced or mitigated through the application of various *measures*. These measures are a non-exhaustive list which includes existing FATF standards, guidance and other measures jurisdictions have haven taken which have proven effective. The GTA is not intended to propose changes to FATF Recommendations, or suggest that jurisdictions go above and beyond FATF standards. These measures are summarised in Annex D.

21. Each chapter of the GTA considers both ML and TF, as often both will use the same features. Where the feature is not largely relevant to one or the other, this is made clear. For example, there are few known cases of TF through complicit gatekeepers (Chapter 5). Each feature consists of numerous sub-features that provide greater specificity. For example, Chapter 2 on cash and bearer negotiable instruments consists of sub-features on cash movements and smuggling, placement, cash intensive businesses and the use of cash as an asset. It is recognised that some of the sub-features could be placed under more than one heading. For example, financial products are listed as a type of asset but can also be used as a means of transferring value. The assessment concludes with an overview of the preceding analysis. It also suggests areas where further action could be taken by the international community.

22. The GTA framework is set out in more detail in Annex A.

1.5. Using the GTA Framework as a Tool

23. The GTA sets out the key ways in which ML/TF components are manifested. This is to assist jurisdictions in the identification of specific threats and their associated vulnerabilities and the application of specific measures to those threats and associated vulnerabilities to combat ML/TF and their negative effects.

24. It is clear that not all of the components described in the GTA will appear equally in every jurisdiction. Similarly the identified harms will vary in degree from jurisdiction to jurisdiction, and so too should the consideration of appropriate measures. Applying the GTA framework in a national or regional context is likely to identify specific *drivers, enablers, harms* and *measures* that have not been captured in the GTA. Users are thus able to draw upon the content of the GTA in line with their specific requirements. For instance, national authorities can apply the GTA framework when conducting geographic assessments, while law enforcement can apply the framework when devising strategies to undermine organised crime groups. In addition, the GTA framework can be used as a basis for joint private/public sector dialogue and by policy makers to review the effectiveness of national AML/CTF regimes. Therefore the GTA also serves as a useful tool to enable the user to examine his or her area of responsibility (whether local, national, or regional), to identify the key components of ML/TF activity.

25. Annex B contains further details on how the GTA framework can be applied at a national or regional level.

1.6. The Overall Harms

26. Criminals go to great lengths to protect themselves and their criminal businesses. Similarly terrorist organisations and individual terrorists expend significant resources to facilitate and sustain their networks. As a result of these actions, the prosperity and security of many are put at risk by today's criminal and terrorist threats.

27. Annex C sets out these harms as they apply to crime and terrorism and cross references them with the type of harm.

The harms associated with money laundering and terrorist financing

28. ML and TF are crucial enablers of the harms caused by crime and terrorism. Finance is the lifeblood of crime and terrorism. Profit is fundamental to the goals of most crime, and therefore criminals make great efforts to move illegally obtained money and other assets in order to convert, conceal or disguise the true nature and source of these funds. The availability of working capital is also fundamental for both criminals and terrorists to sustain their networks. Therefore, the harms caused by organised crime and terrorism will continue to be present as long as criminals and terrorists are able to exploit systems to launder criminal proceeds and to support terrorist groups and activity.

29. Additionally there are distinct harms associated with ML activities. These harms are also significant in social, economic and security terms, and they are often global in nature. On the socio-cultural end of the spectrum, successful ML allows crime to pay, thus encouraging further crime. The economic effects are more wide-ranging, as the activity can have a negative effect on transparency, good governance and accountability of public and private institutions. Laundered money is often untaxed, ultimately depriving countries of infrastructure and social programmes which might otherwise be funded from tax revenue. Also, legitimate businesses can find it difficult to compete with money laundering front businesses that can afford to sell products more cheaply because their primary purpose is to clean money, not make a profit.

30. These harms are illustrative. Later parts of this document aim to set out the harms of ML in greater depth.

1.7. The GTA and the Global Financial Crisis

31. In 2008 the world experienced a financial crisis which significantly harmed the international financial system and as a result also caused variable harms to many individuals, local communities, non-financial businesses and the national and international interests that rely upon the system. ML or TF were not the cause of that harm. Furthermore, there is no evidence to suggest that money launderers and terrorist financiers have changed their behaviour as a result of the crisis, in any significant way to the changes in behaviour of honest citizens.

32. Although observations appear to indicate that the overall turbulence of the recent financial crisis has made it more difficult to identify suspicious activity, the policy responses to the crisis are likely to benefit the global AML/CFT efforts by improving transparency and ensuring more rigorous assurance procedures in the financial system.

33. Where possible, the GTA includes some analysis of the effects of the financial crisis on ML/TF.

1.8. Key Terms

34. The terms *risk*, *threat* and *vulnerability* are often used by the FATF when describing how jurisdictions should implement AML/CFT standards. For example, the FATF has published a number of documents which address the concept of ML/TF risk.[7] However, there is currently no standard or universal definition for these terms.

35. In the context of the GTA, these terms mean:

- ***Threat:*** is a person or thing with an intrinsic potential to pose a danger, cause damage, or cause injury. The abuse of the features identified in this report by criminals and terrorists in an attempt to carry out ML or TF are threats.

- ***Vulnerabilities:*** are the intrinsic properties in a system or structure (including weaknesses in systems, controls, or measures) which make it open to abuse or exploitation by criminal elements for ML, TF, or both. The existence of vulnerabilities in a system makes that system attractive for money launderers and terrorist financers to use.

- ***Risk:*** is the effect of ML or TF activity on the objective of protecting nations, their citizens and their institutions from the harms of profit-motivated crime. The risk manifests when ML/TF threats co-exist with associated vulnerabilities allowing criminals to successfully carry out their ML or TF activity. It is measured as the *likelihood* of ML or TF activity occurring multiplied by the consequences of that occurrence. Thus, the co-existence of threats and vulnerabilities that could result in significant consequences or harms would be considered "high-risk".

1.9. Sources of Information

36. The GTA is based on three main sources of information:

(1) Existing available information, including:

- *FATF and FSRB typologies and mutual evaluation reports:* The findings of the typologies reports developed by the FATF and the FSRBs on individual subjects. In addition, analysis was conducted of 33 mutual evaluation reports of the FATF and FSRB members' AML/CFT systems to identify the major sources of illicit proceeds derived from criminal activity and the significant methods used for ML, TF or both.

- *Surveillance discussion:* The FATF's Working Group on Typologies holds a surveillance discussion three times each year as a regular forum for exchanging information on and examining potential and emerging ML and TF threats. The surveillance discussions have served as a source of information for the GTA.

- *FATF Strategic Surveillance Survey:* The key results of the 2008 and 2009 versions of the survey have been included in this assessment which included responses from 42 and

---

7 FATF (2008), *Money Laundering & Terrorist Financing Risk Assessment Strategies*, FATF, Paris, 18 June.

FATF(2007), *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures*, FATF, Paris, 22 June.

34 jurisdictions respectively. Section 1.2 of this report provides further details on the scope and findings of these surveys.

(2) The results of two typologies workshops involving participants representing more than 30 jurisdictions and international/regional organisations.

(3) In addition there has been consultation with the private sector at a workshop held in May 2009 at the Wolfsberg Forum in Switzerland.

37. This project was conducted by a team of experts from across the globe. They have provided important content, peer review and validation throughout the project with the aim of producing this assessment. Ten countries and eight international and regional organisations were represented: Belgium, the Netherlands (project leader), Russian Federation, South Africa, Spain, Ukraine, United Kingdom (project leader), United States, CFATF Secretariat, GAFISUD Secretariat, GIABA Secretariat (project leader), MENAFATF (Lebanon), Egmont Group of FIUs, International Monetary Fund and the World Bank.

38. The project team would also like to acknowledge the input of many others from government authorities and the private sector whose information and advice was gratefully accepted.

CHAPTER 2: THE ABUSE OF CASH AND BEARER NEGOTIABLE INSTRUMENTS

2.1. Introduction

39. The first feature that money launderers and terrorist financiers abuse prevalently is cash and bearer negotiable instruments. The summary of the 2009 Strategic Surveillance exercise indicated that a noteworthy proportion of ML/TF activity continues to involve cash. The use of cash or currency (*i.e.* banknotes and coins used as a medium of exchange) is attractive to criminals mainly because of its anonymity and lack of audit trail. Criminals look for as much flexibility as possible and are interested in avoiding detection. Cash provides that flexibility, as it is universally accepted and can be used and moved with little or no record keeping.[8] Cash proceeds are often used to purchase further commodities and services. Some criminals also stockpile large amounts of cash as a form of security.

40. Bearer negotiable instruments (BNI)[9] are also attractive to criminals, as they are paper documents which have monetary value to the individual possessing them and are in a form that ownership or title passes upon delivery. Some criminals find it impractical to hold onto huge amounts of cash or BNI and therefore converting cash or BNI into another asset or instrument (*e.g.*, a bank deposit) is often the first stage of the ML cycle. For other criminals, the first stage of the ML process involves converting other assets (*e.g.*, stolen property) into cash in order to be able to launder the proceeds from their crime. ML therefore often involves some form of cash or BNI.

41. In order for terrorists to carry out their operations, attacks or maintain an infrastructure of organisational support, they need to have the ability to collect, receive and move funds. For the same reasons described above, cash provides flexibility for terrorist individuals and groups. By using cash, terrorists are able to stay close to their money without having to place those funds into the financial sector which automatically creates some form of audit trail.

CASH AND THE GLOBAL FINANCIAL CRISIS

The 2009 FATF Strategic Surveillance Survey indicated that an increasing use of cash was identified in some jurisdictions, potentially related to lack of confidence in the financial sector due to the global financial crisis. The crisis has seen significant increases in cash withdrawals and other transactions involving cash, including in countries where financial transactions are primarily conducted electronically. The effect has been to make it more difficult for the private sector to discern between unusual activity by honest actors and suspicious activity which may be related to criminal activity.

---

8 Some currencies are more attractive to launderers and terrorist financiers than others because their universal acceptance is wider. Some currencies are only recognised as legal tender in the issuing country. Other currencies have more widespread acceptance and are more attractive for cross-border laundering and TF.

9 Under FATF Special Recommendation IX (SR IX) on cash couriers the term *bearer negotiable instruments* includes monetary instruments in bearer form such as: travellers cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.

2.2. Major Sources of Proceeds

42. Many of the major sources of criminal proceeds, particularly narcotics trafficking, generate large amounts of cash. Criminals perpetrating some types of fraud tend to avoid laundering cash, preferring instead to purchase goods and pay expenses with cheques and electronic wire transfers. However, identity fraud, access device fraud, and bank fraud can generate large amounts of cash. For example, criminals engaged in access device fraud extract money from cash dispensers/ATMs using stolen ATM card numbers and personal identification numbers (PINs). They then either structure deposits at banks or undertake wire transfers through money remitters. This activity is similar to that which is sometimes carried out by those laundering the proceeds of narcotics trafficking. Other criminal activity which can generate large amounts of illicit cash include, but are not limited to, smuggling, corruption, bribery, extortion and illegal gambling.

43. The major sources of TF are from both illicit and legitimate sources, and the nature of the funding sources may vary according to the type of terrorist organisation. In many of these cases, cash is either generated or collected. For example, a number of terrorist groups engage in criminal activity such as narcotics trafficking, kidnapping and robbery or theft to generate cash income. Legitimate sources of funding such as charitable donations and the establishment of a legitimate business also produce cash proceeds. These cash funds are then used for travel, training, staging attacks and the acquisition of weapons or explosives.

2.3. The Sub-Features

44. The following sections consider the harms associated with abuse of the following sub-features of cash and bearer negotiable instruments:

- Cash movements and smuggling,
- Placement (including third party accounts).
- Cash intensive businesses.

45. Each of the sections describes the harms specifically arising from the sub-feature, the drivers behind criminal and terrorist abuse and the enablers that allow the criminal or terrorist to take advantage of them. Finally, consideration is given to some of the measures that can be taken to allow countries to address the drivers and enablers and so reduce the harm caused. Countries may wish to consider these and other options in designing their AML/CFT strategies.

2.3.1. Cash Movement and Smuggling

46. The findings of the 2009 FATF Surveillance Survey show that globally, the physical movement of cash within jurisdictions and cash smuggling across borders are consistently used to move the proceeds of crime and play a significant role in financing of terrorism. As more AML/CFT controls are placed on financial sector, criminals look at alternative means to move their illicit cash.

47. Cash smuggling can be subdivided into two categories. These are (1) bulk cash smuggling (BCS) and (2) cash couriers. BCS involves large volumes of cash which represent the proceeds of crime. Methods generally include the use of land or sea border crossings through concealing cash in vehicles or containerised cargo. Cash couriers are natural persons who physically transport cash on their person or accompanying luggage. This method is also associated with TF, as it involves smaller amounts than BCS. The preferred methods for cash couriers are commercial airlines, and new cases have highlighted the use of

private planes. In addition to the air, sea and land methods referenced above, mail services have also been used to smuggle cash.

48. Illicit cash is sometimes smuggled using larger denomination notes, as it reduces both the size and weight of the load[10]. For this reason, some criminals choose to exchange small denominations for larger denominations before smuggling the cash, typically by using the services of a money service business. Changing cash into larger denominations can also reduce the forensic evidence available from any seized cash: The higher denominations, particularly when sourced from a money service business, will not have had the same exposure to illicit substances as the cash that criminals collect from users to purchase the commodity. Most airlines have weight limits for both carry-on and a checked-in baggage. Because of its bulk and weight, the challenge in moving bulk cash is either to use large containers (*e.g.*, commercial shipping containers or specialised compartments in vehicles) or split it up among many couriers. Using many couriers has the added advantage of mitigating the risk of loss should one or more couriers be stopped.

49. Case studies[11] from around the globe demonstrate that many of the ingenious methods used to smuggle illicit narcotics have also been used to smuggle cash or bearer negotiable instruments across borders.

Harms

50. There are a number of specific harms resulting from illicit movement of physical cash and cash smuggling by criminals and terrorists. These include robbery and risk of violence between criminals. Mechanisms that allow criminal cash to be moved and value to be transferred also fund further criminal and terrorist activity. The ability to use illicit cash allows a profit from crime to be realised. Funds held in cash are also less likely to be available to be taxed by the authorities. The use of this sub-feature removes currency from active circulation in the country where the criminal activity takes place and may also increase demand for and the cost of issuing currency.

Drivers

51. Criminals and terrorists try to achieve a number of objectives by physically transporting or smuggling cash. Primarily, they attempt to avoid preventive measures in the host financial sector. Criminals and terrorists also seek to move funds in a form that is both familiar and comfortable for them. They also try to distance proceeds from the location of crime. Both criminal and terrorist activity generate and require cash. Smuggling cash ensures the security and retention of value by staying outside of the financial system and away from financial products. By using this sub-feature, the criminal or terrorist can stay close to his money, many foreign destinations can be quickly reached and little pre-planning is required.

---

10 For example, a briefcase measuring 10x39x50 cm would hold value of EUR 7.4 million in EUR 500 notes, weighing 14.8 kg (14 800 notes). The same briefcase would hold GBP 740 000 (EUR 740 000, rate of exchange 1:1 as at March 2010), in GBP 50 notes, only 10% of the value, or USD 1.48 million (EUR 2.22 million, rate of exchange 1:1.5 as at March 2010) in USD 100 bills.

11 FATF (2010) *Detecting and preventing the illicit cross-border transportation of cash and bearer negotiable instruments: International Best Practices*, FATF, Paris.

Enablers

52. Cash is universally accepted and allows portability and flexibility when transferring value. High denomination notes are easily available in some jurisdictions. Such notes reduce volume and therefore increase portability.

53. The lack of reporting requirements and preventive measures in some areas makes the abuse of this feature attractive. For example, in relation to BNIs in certain countries, travellers are not required to declare travellers' cheques when exiting their country. There is also low reporting and weak regulation within sectors which provide cash. The anonymity and lack of audit trail of cash provides further flexibility to the criminal or terrorist. Lastly, funds generated outside the financial system and kept outside the financial system help avoid detection.

Measures for consideration

54. FATF Special Recommendation IX (SR IX) contains deterrent and institutional measures that jurisdictions should take to address the illicit movement of cash internationally. Special Recommendation IX also contains provisional measures and confiscation procedures (in line with Recommendation 3 and Special Recommendation III), as well as measures related to international co-operation.

55. While not in the Special Recommendation IX definition of a "bearer negotiable instrument", countries could consider adopting a regulation providing for obligatory declaration of travellers' cheques when travelling abroad. Countries have also considered including reporting requirements for other forms of value (*e.g.*, gold coins, casino tokens and access devices) which currently fall outside the scope of the FATF definition of BNI.

56. The issue of cash couriers and BCS has been referred to in numerous FATF annual typologies reports from 1998 to 2002. In addition, the FATF issued international best practices on "Detecting and preventing the illicit cross-border transportation of cash and bearer negotiable instruments" in 2010. These best practices focus on areas that have proven to be challenging for jurisdictions to implement and provides tested solutions. For example, the guidance includes a list of red flag indicators that could be used to detect cash couriers and asks countries to consider not issuing large denomination bank notes.

57. Many low capacity countries are cash-intensive economies. Therefore, strengthening financial inclusion in those countries could be considered to reduce the severity of the risk of cash.

2.3.2. Placement (including Third Party Accounts)

58. The placement of illicit cash into the financial sector including through DNFBPs is one of the most common and easily detected forms of ML activity. Cash, though anonymous, does attract attention when used in certain situations and can create an audit trail. As large cash transactions (for example, depositing cash into a bank or purchasing high-value goods) might prompt reporting by a financial institution or DNFPBs, criminals will structure their cash deposits using a series of small amounts and using multiple accounts. For example, criminals have been known to place available cash in bank and short-term deposit accounts in different banks and then to replenish these deposit accounts. These seemingly unrelated petty cash deposits are later withdrawn in cash (through an ATM anywhere in world), exchanged for another currency and transferred overseas, or converted to another form of value. In many cases, criminals will use third party accounts. Third party accounts are often created under the name of a family member, associate or legal entity. For example, access to an account may be granted to a third party

upon presentation of the account holder's details (account number, name of the account holder), an identification document, or the power of attorney.

59. With respect to TF, funds are often kept out of the financial system to avoid detection. Some jurisdictions indicate the use of the formal financial sector for TF is low or decreasing. However, regular funding to maintain a terrorist group's capacity can be conveniently facilitated via the placement in the conventional banking system, and some jurisdictions have indicated that the banking sector is the most common venue for placing terrorist funds and then moving them.[12] In one example, terrorists placed large cash deposits into financial institutions to secure the rental of a building.

60. The 2009 Strategic Surveillance exercise found that in both ML/TF cash deposits (and withdrawals) associated with transfers (using financial institutions or remittance services) continue to be an important aspect. The 2009 survey also reported that one jurisdiction had witnessed the use of transit points in TF transactions whereby third parties, located in third countries, received the initial transfers and forwarded these to the ultimate recipients. Transfer of value is dealt with in Chapter 3.

Harms

61. There are a number of specific harms resulting from the placement of cash for ML/TF purposes, including third party accounts used by criminals and terrorists. There is an increased risk of robbery if businesses and individuals are holding and transporting increased levels of cash. The placement of illicit cash also provides a competitive advantage to complicit business.

62. Placement often takes place through the use of false or stolen identities. Mitigating action by governments against identity fraud requires significant resources and costs, which increase with the sophistication of identity fraud methods. Placement of criminal cash also allows a profit from crime to be realised. Finally, the widespread use of false and stolen identities could result in a lack of confidence in public sector and financial sector data-sets and processes.

Drivers

63. Criminals and terrorists try to achieve a number of objectives through the use of placement, including through the use of third party accounts. Mainly they need to get cash into the financial system without detection by the authorities. The use of accounts ensures the safety and easy access to funds. Criminals do not want limits on their ability to operate and live entirely on a cash basis, particularly in developed economies.

Enablers

64. Structuring cash by opening cash deposit accounts in various banks makes it possible to avoid scrutiny from law enforcement and oversight bodies. Criminals have access to numbers of individuals who are willing to conduct placement activity for little reward. Good international communications exists to co-ordinate placing and transfer of value.

65. In addition, criminals have the possibility of transferring the right to access bank or deposit accounts to third parties, but some regulations do not always require customer due diligence (CDD) on third party depositors. Regulations also can set high thresholds for reporting cash transactions in some cases.

---

12 See: FATF (2008), *Terrorist Financing Typologies Report*, FATF, Paris, 29 February, p. 21.

66. Finally, criminals and terrorists will use false or stolen identities to open accounts to facilitate placement while avoiding being identified by CDD requirements.

Measures for consideration

67. There are a number of wide-ranging preventive or deterrent measures contained within the FATF standards that are applicable to this sub-feature. These measures focus on CDD, record keeping and the reporting of unusual, suspicious or large-value transactions (*e.g.*, Recommendations. 5, 9-11, 13, 19 and Special Recommendation IV). As described throughout this chapter, criminals and terrorists use cash to remain anonymous and to avoid detection. The creation of an audit trail is considered one measure to assist authorities in revealing the true source and ownership of the cash. Where terrorist funds are derived from criminal activity, then traditional monitoring mechanisms that are used to identify ML may also be appropriate for TF although the activity, while suspect, may not immediately be identified as connected to TF.

68. To complement the FATF standards, some jurisdictions have taken additional measures, such as providing additional powers to law enforcement authorities, including the use of geographic targeting orders (GTO). A GTO provides regulators with the authority to require a financial institution or a group of financial institutions in a geographic area to file additional reports or maintain additional records beyond the ordinary AML/CFT reporting requirements. This is particularly useful when a specific sector or area has been identified where illicit cash proceeds are being placed to avoid AML/CFT reporting requirements. It serves as an information gathering device that enables law enforcement authorities to gain greater knowledge of patterns of ML and also helps to prevent evasion of AML/CFT regulations by disturbing established patterns of ML through the introduction of uncertainty and heightened risk into criminal and terrorist decision-making.

69. A further optional measure developed by the project team might be to require CDD on occasional transactions. This could be applied on a risk-sensitive basis, irrespective of the amount involved. The issue of when financial activity is carried out by a person or entity on an occasional or very limited basis is dealt with in the 2007 *FATF Guidance on the Risk-Based Approach (RBA) to Combating Money Laundering and Terrorist Financing: High Level principles and Procedures*.

70. At the same time, financial inclusion, particularly in low capacity countries should be encouraged to reduce the severity of the risks related to cash. This also implies that unnecessary administrative burdens should be avoided, depending on the risks of different products.

2.3.3. Cash Intensive Businesses

71. The use of retail and service businesses such as restaurants, pubs and convenience stores have long been used by criminals to facilitate the laundering of illicit cash. These legitimate businesses are sometimes referred to as “front companies” if they are set up to provide plausible cover for illegal activities. Non-cash based abuse of corporate front organisations or “shell companies” and terrorist front organisations are discussed in Chapter 3.5 of this report.

72. The involvement of cash intensive businesses was identified as a risk factor in the 2009 Strategic Surveillance responses. For example, some jurisdictions saw increased injections of illicitly derived cash into otherwise legitimate businesses. Cash intensive businesses can be used during all stages of the ML cycle, especially the placement stage. Criminals will establish business accounts to deposit large volumes of cash in low denominations as daily earnings. In many cases, no legitimate transactions take place at the business. When legitimate commerce does take place, the illicit money is commingled with the legitimate earnings, thus disguising the true source of the funds.

73. With respect to TF, the proceeds from a legitimate cash-intensive business can be used as a source of funds to support terrorist activities, and this was highlighted as one of the main reported licit sources of funding for terrorism in the surveillance exercise. A wide range of types of businesses were highlighted including those in the construction industry, used motor vehicles traders, travel agencies, gold and jewellery stores, currency exchange offices, clothing stores, butchers, sandwich bars and associations. These businesses can direct funds to terrorist organisations/activities when the relation between sales reported and actual sales is difficult to verify. There have been a number of cases identified of terrorists buying out or controlling cash-intensive businesses including, in some cases, money services businesses to move funds.

74. Casinos are by their nature considered cash-intensive businesses, as the majority of transactions are cash-based. In March 2009, the FATF published a report on ML vulnerabilities in the casino and gaming sector. The report showed that there is significant global casino activity which is cash-intensive, competitive in its growth and vulnerable to criminal exploitation.

Harms

75. There are a number of specific harms resulting from the use of cash-intensive businesses by criminals and terrorists. Competitive advantage is given to complicit business. Placement of criminal cash allows a profit from crime to be realised. Through the use of businesses criminals may corrupt (wittingly or through coercion) others employed in these businesses.

Drivers

76. Criminals and terrorists try to achieve a number of objectives through the use of cash-intensive businesses. Mainly, they want to conceal source of illicit funds by mingling them with legitimate funds. Criminals and terrorists want to provide value for money by creating economies of scale (*i.e.* cash-intensive businesses are an easier way to get large amounts laundered than through personal accounts). Ownership of business permits the acquisition of community standing and influence, which provides additional cover for illicit activities. In addition, proceeds of legitimate business can be used as a source of funds to support terrorism.

Enablers

77. Criminals and terrorists are able to take advantage of cash-intensive businesses. Using this sub-feature enables placement of cash with less risk of detection than if conducted by individuals. The regulated sector is more likely to consider large sums as normal when a business is involved. Cash-intensive businesses are also able to inflate how much legitimate cash comes in each day to disguise the deposit of cash from criminal activity.

78. In some countries awareness and scrutiny of cash-intensive businesses by the authorities is minimal. It is also difficult for financial institutions to monitor the accounts held by these businesses.

Measures for consideration

79. FATF Recommendations 12, 16 and 24 extend controls to DNFBPs including dealers in precious metals, dealers in precious stones and casinos. In addition, Recommendation 19 asks jurisdictions to consider implementing a system in which financial institutions and intermediaries report all domestic and international currency transactions over a fixed amount or large-value cash transactions. These Recommendations can be particularly useful if a country has a specific sector which faces a ML or TF threat. Also, Recommendation 20 requires that consideration to be given to extending regulation to other businesses and professions, including cash-intensive businesses, if they are at risk. Tax authorities could

also play a role in detecting abuse of cash-intensive businesses in the context of fiscal scrutiny and auditing activities.

80. Casinos are generally subject to a range of regulatory requirements, commercial considerations, and security measures, which can complement AML/CFT measures. For example, the use of surveillance in casinos reduces the severity of the risk of chip-based ML schemes, in which criminals hold chips for a period of time and later cash them in for a casino cheque. In October 2008, the FATF published guidance on the risk-based approach for casinos.

CHAPTER 3: THE ABUSE OF TRANSFER OF VALUE

3.1. Introduction

81. The second feature that money launderers and terrorist financiers abuse prevalently is the transfer of value (this does not include cash or bearer negotiable instruments, which are dealt with in Chapter 2). The transfer of value remains central to the functioning of the global economy and is a natural process in any financial transaction. On a daily basis, millions of global transactions facilitate the transfer of value through the use of the financial system, money transfer businesses and systems, the international trade system, third party business structures, charities, remittance systems and new payment methods. The vast majority of these transactions are legitimate. The challenge is to distinguish legal from illegal use of transfer of value.

82. Criminal proceeds are often not in the place or form that the criminal requires. He must therefore employ a process whereby illegally derived profits are layered through various transactions for purposes of re-integration into the legal economy or to allow the funding of further criminal activity. The tactics that the criminal adopts will depend on his requirements which will in turn be determined by a number of factors – the physical location of the funds, the form they are in, what he wants to use the funds for (financing further criminal activity, direct spending to support his lifestyle, long term laundering for later use etc.) and the local conditions (levels of enforcement and regulation). However, there will be one distinct need common to most criminals. He will want to distance the proceeds of the crime from the crime itself in order to protect himself from detection and likely prosecution. [13]

83. For terrorists, and those facilitating the financing of terrorism, the immediate aim is different, but the mechanisms they use are effectively the same. Rather than trying to distance the funds from the crime, terrorists will want to move money undetected from the source of the fundraising activity to the location of the group or persons that will carry out the terrorist activity. This may be a physical distance, in the case of fundraisers in one location supporting activity in elsewhere, or it may involve moving legitimate income to allow the purchase of goods or services, for example, to provide general support to a terrorist or group of terrorists or to directly finance a terrorist act.

3.2. Major Sources of Proceeds

84. ML associated with all predicate offences is likely to require the transfer of value at some point as is the case in most TF cases. The 2009 FATF Strategic Surveillance Survey noted that a number of jurisdictions have seen this feature used to facilitate various ML schemes involving fraud and tax or excise evasion.

---

13 The range of the required distance will depend on such factors as the risk of detection at the location of the crime and the criminal's appetite for risk.

3.3. The Sub-Features

85. The following sections consider the harms associated with abuse of the following sub-features of the transfer of value**:**

- The banking system.
- Money transfer businesses and alternative remittance.
- The international trade system.
- Third party business structures, charities and other legal entities.
- Retail payment systems and the ATM network.

86. Each of the sections describes the harms specifically arising from the sub-feature, the drivers behind criminal and terrorist abuse and the enablers that allow the criminal or terrorist to take advantage of them. Finally, consideration is given to some of the measures that can be taken to allow countries to address the drivers and enablers and so reduce the harm caused. Countries may wish to consider these and other options in designing their AML/CFT strategies.

3.3.1. The Banking System

87. The transfer of value feature often relies on banking structures to a greater or lesser degree. Even where the true, laundered, value is transferred indirectly via goods and services (see Section 3.3.3. on abuse of international trade system), these systems are often used to reconcile the relevant accounts. The banking system is also often used to transfer value even when launderers utilise other methods or features such as those available in the securities and insurance sectors.

88. Bank transfers allow value to be moved electronically and relatively quickly in a relatively highly regulated environment. It is a high volume activity, with millions of legitimate transactions taking place globally each day across thousands of banks, involving an even greater number of counterparties. Access to the banking system can be over the counter, or by using the internet or telephone, by the owner of the funds or by instructed third parties, such as lawyers, accountants or private bankers.

89. The 2009 FATF Strategic Surveillance Survey noted wire transfers involving cash deposits and withdrawals as a primary technique for moving terrorist funds. The 2009 survey also noted that the financial systems in a number of jurisdictions have been used as a part of a train of transactions, with funds liked to terrorism moving in and then directly out of their countries.

Harms

90. The abuse of the banking sector to transfer value by criminals and terrorists can undermine confidence in the integrity of the financial system and damage the reputation of the system and businesses within it, with the potential result in damage to business, markets and even whole economies. This can drive away legitimate business and make institutions more reliant on criminally sourced funds. An additional harm would be the difficulty of tainted institutions' gaining access to the global financial sector.

91. Abuse of the banking system is often enabled by identity fraud. Mitigating action by governments against this requires significant resources and costs, which increases with the sophistication

of identity fraud methods. Widespread use of false and stolen identities to access the banking system could also result in a lack of confidence in public sector and financial sector data-sets and processes.

Drivers

92. The factor that drives criminals and terrorists to use the banking sector to transfer value for ML/TF is their need to move funds securely, quickly and with the appearance of legitimacy. There is also a need to convert funds into various other products and to move funds away from predicate offences. Another identifiable driver is the need to move funds to where they may be needed / accessible including for the commission of more criminal activity or to separate funding for terrorist logistics from other funds.

93. Funds are also transferred to locations with weaker AML/CFT regimes because the activity is less likely to be identified, reported and investigated, while the proceeds are less likely to be confiscated and offenders less likely to be prosecuted (see Chapter 6 for further detail on the drivers for abuse of particular jurisdictions).

Enablers

94. The abuse of the banking sector is enabled by factors such as the sheer size and scope of the global financial sector, complexity of banking arrangements and products which allows concealment. Banking systems in those jurisdictions with weak preventive measures also enable the abuse of this sub-feature.

95. The abuse of the banking system is often also enabled by the use of false or stolen identities which are used to avoid being identified through application of CDD requirements or to gain access to accounts.

96. Another enabler is the possibility of transferring the right to access bank/deposit accounts to third parties. In some cases access to an account may be granted to a third party upon presentation of the account holder's details (account number, name of the account holder), an identification document and the power-of-attorney. Also customers' ability to remotely access deposited funds means that illegal funds integrated into the banking system can be managed without the physical presence of the account owner, through a bank-customer system (operated via the internet or telephone) from virtually any place of the world. When a bank's internal control service detects a suspicious transaction, getting in touch with the customer to clarify the nature and goal of the transaction may be difficult. The bank's customer, being physically far away from the bank, may continue to conduct the suspicious transactions remotely before access is eventually discontinued.

Measures for consideration

97. The most important measures for mitigating the ML/TF threats relating to the transfer of value associated with the misuse of the banking system are those set out in Recommendations 5 and 11 and Special Recommendation VII which require customer identification, the monitoring of transactions by financial institutions and the inclusion of meaningful and accurate originator information with funds transfer. For the latter, beneficiary financial institutions should take measures to identify wire transfers that are not accompanied by complete originator information. A related issue involves cover payments, which are used to facilitate funds transfers on behalf of a customer to a beneficiary in another country, and typically involve the originator's and beneficiary's banks not having a relationship with each other that allows them to settle with each other directly. The FATF released a statement[14] on cover payments in

[14] See: FATF (2009), *Chairman's Summary, Paris Plenary, 14-16 October 2009*, FATF, Paris, 16 October.

October 2009 to address the potential for misuse of cover payments and to promote greater transparency of cross-border wire transfers.

98. Further measures include freezing and blocking bank and deposit accounts in line with Recommendation 3 and Special Recommendation III. These measures relate to the transfer of value in that effective freezing mechanisms result in the termination of terrorist cash flows by shutting down the pipelines used to move terrorist related funds or other assets[15]. These measures also force criminals and terrorists to use more costly and higher risk means of financing their activities, which makes them more susceptible to detection and disruption. Furthermore, these measures are efficient as they deprive the criminal of the funds acquired by criminal methods and undermine the financial basis for criminal activities.

99. Some countries have considered adopting laws authorising or requiring banks to deny opening an account to certain customers including criminals. This can deny access directly or even indirectly, for example by preventing criminals from opening bank accounts in the name of companies registered under lost or other people's documents. However, in some countries this is not possible.

Emerging issue – money mules

Law enforcement is increasingly seeing the use of "money mules" as a new means of transferring value. This is reflected in the results of the 2009 FATF Strategic Surveillance Survey. Money mules are used to launder the proceeds of fraud schemes (*e.g.,* phishing and identity theft). Criminals who gain illegal access to deposit accounts recruiting innocent third parties to act as "money mules." In a money mule transaction an individual is recruited to receive and then send wire transfers from deposit accounts to individuals overseas, minus a certain commission payment (perhaps between 5-10%).

Money mules are recruited by a variety of methods, including spam e-mails, advertisements on genuine recruitment web sites, social networking sites, instant messaging and advertisements in newspapers. Once recruited, money mules will receive funds into their accounts. Mules are then asked to take these funds out of their account and to forward them overseas (minus the commission payment).

As well as the harm caused to the victims of the fraud, when caught, money mules often have their bank accounts suspended, causing inconvenience and potential financial loss.

3.3.2. Money Transfer Businesses and Alternative Remittance Systems

100. In addition to the use of the banking system, criminals and terrorists will also use non-banking structures or structures that mix both. Although there are differences between them[16], money transfer businesses and alternative remittance systems (MTB/AR) are both retail financial services that allow for value to be transferred. In some cases, the use of such services is supported and facilitated by historic and cultural links. Some businesses are global franchises that allow value to be transferred almost anywhere in the world. Other businesses service a more limited community or group[17]. The 2009 FATF Strategic

15 See: FATF (2009), *International Best Practices: Freezing of Terrorist Assets (Special Recommendation III)*, FATF, Paris, 2 July.

16 Money transfer businesses can either use their own propriety systems or existing banking systems, while alternative remittance systems do not use existing banking systems. In some jurisdictions and regions these services are the primary means of transferring value.

17 In recent years the FATF and FSRBs have undertaken substantial work this issue: FATF (2003), *International Best Practices Paper on Combating the Abuse of Alternative Remittance Systems* and FATF (2003), *Interpretative Note to Special Recommendation VI: Alternative Remittance*; Asia Pacific

Surveillance Survey noted that a number of jurisdictions are seeing increasing abuse of alternative remittance systems. One jurisdiction provided a detailed description of "cuckoo smurfing" which uses alternative remittance systems and involves innocent parties and those innocent parties' accounts without their knowledge.

101. The 2009 survey also noted two variations in terms of the involvement of alternative remittance systems for TF purposes. One respondent observed the use of online remittance services where the remittance company used *nostro* (correspondent) accounts, resulting in relatively limited information existing concerning the transaction. Another observed transactions where the person obtained a bank draft in favour of a money service business.

Harms

102. Crucially, mechanisms that allow criminal cash to be moved and value to be released, fund further criminal and terrorist activity. They also allow a profit from crime to be realised.

103. The abuse of this sub-feature also undermines confidence in the integrity of these businesses and damages the reputation of the system and businesses within it. The use of these methods in preference to the banking sector, undoes the benefit of controls applied by the banks. It can also be enabled by the use of false or stolen identities. Mitigating action by governments against this requires significant resources and costs, which increases with the sophistication of identity fraud methods.

104. ML/TF through MTBs/AR can result in the need for additional and stricter controls with the effect that some of these businesses either move underground, close down or the extra cost is passed on to genuine customers who are often already disadvantaged.

Drivers

105. Various factors that drive criminals and terrorists to use MTBs/AR include the need to place cash and move its value quickly and outside of the banking sector, including in high volumes. The use of these allows for access to locations where the banking system is not present. Funds can be moved quickly, cheaply and securely using trusted and personalised arrangements. These systems are also abused to avoid currency control restrictions as well as existing AML/CTF controls in the banking sector.

Enablers

106. Criminal and terrorist use of MTBs/AR to transfer value is enabled by various factors. It is characterised by variable regulation and application of controls. In some jurisdictions, there is even a total absence of controls or oversight for this sector.

107. Access to these businesses may be more convenient than to the formal sector, both to remitter and receiver. The remitting business often has links with both sender and receiver, including cultural links, trust, geographic links or complicity.

Group (APG) (2003), *Alternative Remittance Regulation Implementation Package*; Middle East and North Africa Financial Action Task Force (MENAFATF) (2005), *Best Practices on Hawalas*; FATF (2009), *Risk-Based Approach Guidance for the Money Service Business Sector*; FATF and MONEYVAL (2010), *Money Laundering through Money Remitters and Currency Exchange Providers*.

108. Vulnerable business models/small businesses mostly cannot support sophisticated AML/CTF control systems while sole traders have no management or compliance oversight obligations.

109. These businesses are generally more cash intensive than banks and one-off transactions attract less attention. Unregistered money transmitters may retain records that are in a form which investigators cannot easily scrutinise and regulators cannot easily monitor.

Measures for consideration

110. The key measures to counter the ML/TF threats relating to the transfer of value, associated with the misuse of money transfer businesses and alternative remittance services are those set out in Special Recommendation VI. These measures are based on the premise that all providers of such services should operate within a controlled environment where, at a minimum, they are required to register or obtain a license to carry on a money transfer business. Another core element for Special Recommendation VI is that the money or value transfer services be subject to the applicable FATF Recommendations (*i.e.* Recommendations 4-16 and 21-25). Lastly, Special Recommendation VI requires jurisdictions to impose sanctions on money/value transfer services that operate without a license or registration and that fail to comply with the relevant FATF standards.

111. However, the implementation of these measures must take account of the differences in nature between providers of these services and other financial sectors such as banking and must be balanced with objectives such as the provision of basic financial services to persons who do not have access to formal financial institutions. More generally, authorities could also consider what they can do to make the use of the formal sector more attractive (*e.g.*, take steps that reduce transaction cost).

112. SR VII on wire transfers is also relevant to these businesses. This is covered in more detail in the Section 3.3.1. on the banking system.

113. In June 2003, the FATF issued an best practices paper on combating the use of alternative remittance systems. This included a number of measures that can be considered.

114. In addition, countries have highlighted the importance of ensuring that law enforcement and regulatory agencies work collaboratively to identify and prosecute these businesses that facilitate ML. Where there are prosecutions or other law enforcement or regulatory action, publicity around this can have a multiplying effect in encouraging compliance or discouraging criminal activity. In this respect, the guidance issued by the FATF and FSRBs (*e.g.*, APG and MENAFATF) contains practical identification strategies.

115. Steps to increase the transparency of money transfer businesses and alternative remittance systems are also worth considering. This includes beneficial ownership, as often criminals will put forward relatives or associates to nominally run the business, in order to avoid scrutiny. Other measures worth consideration include limitations on the amount of businesses in certain areas.

Transfer of value and the global financial crisis

The crisis has brought a potential for financial activity in some countries to increasingly go to areas of the financial sector that are sometimes considered to be outside of the mainstream or banking sectors This is because services offered can sometimes be cheaper such as, for example, the services of MTBs/ARS. In countries where there is

less transparency or regulation of these areas this may add to the risk.
In addition a trend towards getting loans for "alternative" sources has been observed as it has become more difficult to get loans from financial institutions. The provision of such loans can be undertaken by criminal groups and presents them with opportunities to launder and obtain yet further illegally obtained funds[18].

3.3.3. The International Trade System (including Trade Based Money Laundering)

116. The international trade system is used to move money and goods in large amounts and governments have limited scrutiny to counter its illicit side. The international trade system can be abused through tax avoidance and evasion, capital flight and trade-based money laundering (TBML). This abuse has been studied by the FATF who issued a typologies paper in 2007 on TBML. The 2009 FATF Strategic Surveillance Survey also noted the use of the international trade system for both ML/TF purposes.

117. TBML refers to the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origins or finance their activities. This can be accomplished through misrepresentation of price which as well as with overpriced or underpriced invoices. Similarly, the quality or quantity of goods can be misrepresented.

118. Alternatively, entirely legitimate trade can be used to move value. In this case, debts incurred with legitimate companies are placed under control of the money launderer. These debts are then settled using value received from criminal groups, mostly located in third countries. The company may not be aware of the true source of the funds used to settle the debts.

119. A further type of TBML relates to laundering associated with value added tax (VAT) or *carousel* fraud. An FATF typologies report on this was issued in February 2007. In such cases, money flows take place which may or may not be supported by movements in goods. These are often undertaken through the banking sector.

120. In June 2008 the FATF published a typology on proliferation finance which provides detailed information on trade finance (it should be noted that the broader context of proliferation finance is outside the scope of this report). In addition, an FATF typology on free trade zones (FTZs) was published in 2010, which also covers issues related to the international trade system and TBML.

Harms

121. Specific harms resulting from the abuse of the international trade system, including TBML, to transfer value by criminals and terrorists include that it can jeopardise the credibility and reliability of international trade. This activity can also undermine the stability of countries' borders and financial systems.

122. Vulnerabilities allowing this abuse can also create opportunities for evasion of duties, tariffs and taxes which result in the loss of legitimate government revenue. It also allows capital flight and/or the evasion of currency restrictions.

---

18 A presentation by the Japan Financial Intelligence Centre to the FATF Working Group on Typologies in October 2009 showed how organised crime in Japan is increasingly using loan sharking as a source of funding.

Drivers

123. The factors that drive criminals and terrorists to use the international trade system to transfer value include the wish to move value with the appearance of legitimate trade thus avoiding attention and preventive measures.

124. Another need is that the international trade system allows for large-scale laundering over the long term. Proceeds can be integrated into otherwise legitimate businesses which are involved in trade. The predicate offence and the individuals involved in them thus remain distanced from the activity.

125. Inherent vulnerabilities in the international trade system, such as the enormous volumes of trade flow, provide opportunity for criminals and terrorist groups to transfer value across borders.

Enablers

126. AML/CFT measures have been developed with traditional financial sector practices in mind and have not been built around trade finance, whereas understanding of TBML is still immature in public and private sectors. Criminal and terrorist use of the international trade system to transfer value is enabled by factors such as the fact that corporate structures which are lacking transparency make it easier to obscure beneficial owners of funds.

127. The volume of trade not only has the potential to hide individual transactions, but makes oversight and enforcement difficult. The complexity of international trade also makes it difficult to match payments to value. The various means used to physically move goods – for example by boat, plane, road and rail – enable criminals to diversify their delivery channels and thus evade detection.

Measures for consideration

128. None of the FATF Recommendations currently call for specific measures to facilitate the detection and investigation of ML/TF through the trade system. The FATF issued a non-binding best practice paper on TBML (20 June 2008) with the objective of improving the ability of competent authorities to collect and effectively utilise trade data for the purpose of detecting in a risk based manner and investigating ML/TF through the trade system. The 2010 typologies report on free trade zones (FTZs) also suggests a number of areas for consideration which include how the FATF standards and preventive measures can best be applied within FTZs. There is a particular need to create gateways, mechanisms and channels to improve national and international co-operation with competent authorities as well as with the private sector. The exchange of information is a key element to better identify the illicit activities (*e.g.*, fraud schemes*)* using FTZs.

129. The following measures are worth consideration:

- Ensuring that financial institutions, especially the global trade services departments have training programs to strengthen their trade finance policies and activities.
- Establishing programmes to build expertise and raise awareness with trade, investigative, prosecutorial and regulatory authorities to identify TBML techniques.
- Disseminating typologies, red-flag indicators and sanitised case studies to private sector and competent authorities.

- Developing domestic mechanisms to link investigative authorities with those responsible for collecting and storing trade data.

- Establishing clear and effective gateways to facilitate the international exchange of trade data amongst authorised counterparts. Considering establishing a *trade transparency unit*.

- Requirements for transparency between goods and value for financial service providers (*i.e.*, banks see import documentation as well as invoices).

- Sharing information with domestic and foreign agencies (with specific emphasis on import and export information), and then acting on this.

- Providing sufficient training and cross learning to the various parties to result in unified and common responses.

3.3.4. Third Party Business Structures, Charities and Other Legal Entities[19]

130. Criminal and terrorist funds can be moved to a variety of third party business structures before being moved further on. Such business structures include various corporate vehicles, such as limited companies, partnerships, or publicly traded businesses.[20] Trusts are a further type of legal entity or arrangement which may be used to facilitate the movement, integration and structuring of funds. Respondents to the 2009 FATF Strategic Surveillance Survey consistently highlighted risks associated with shell or front companies. The 2009 survey also noted that many jurisdictions are now seeing the use of trusts and other complicated company structures which make it difficult to determine the real and beneficial owners.

131. In addition, charities and NPOs can be used as vehicles through which funds can be pooled and then transferred to where they can be used, in particular by terrorist financiers[21]. The misuse of the NPO sector was highlighted by many jurisdictions in the 2009 survey. For example, jurisdictions observed the collection and transmission of funds using the accounts of NPO officers.

132. Such entities can be existing structures that the criminal or terrorist is able to misuse, or one that has been deliberately set up to allow ML/TF to take place. Of particular concern is the ease at which corporate vehicles can be created and dissolved in some jurisdictions, which allows these vehicles to be used not only for legitimate purposes (such as business finance, mergers and acquisitions, or estate and tax planning) but also to be misused by those involved in ML/TF to conceal sources of funds and their ownership of the corporate vehicles.

133. The 2008 FATF typologies report on terrorist financing also identified the establishment and use of mass media outlets or publication companies by terrorist organisations in a number of jurisdictions, particularly in Europe. These companies have been used not only as a method of transmitting funds but

---

19 This sub-feature is closely related to the use of professionals and insiders which is located in Chapter 5 on Gatekeepers.

20 A detailed FATF typologies report on the misuse of corporate vehicles was published in October 2006 and contains relevant case studies. It furthermore identifies risk factors associated with corporate vehicle misuse and suggests a number of areas that may call for further consideration in preventing such misuse.

21 See: FATF (2008), *FATF Terrorist Financing Typologies Report*, FATF, Paris, 29 February.

also as a source of funding, to collect money and as a meeting point to promote propaganda and facilitate TF.

Harms

134. The abuse of third party business structures, charities and other legal entities damages the reputation of legitimate businesses and sectors. The charitable sector, in particular, is vulnerable to its reputation being eroded. This in turn might have a negative impact on the levels of charitable donations. For example, the possible diversion of legitimate funds from charitable work to fund terrorists also discourages citizens from donating to charities.

135. Abuse of this sub-feature can also be enabled by use of false or stolen identities. Widespread use of false and stolen identities can result in a lack of confidence in public sector data-sets and processes.

136. In the event that such corporate vehicles are available for investment, opaque structures can hinder the ability of counterparties to assess the risk of investments. This in turn can hinder integrity, asset quality, soundness and stability[22].

Drivers

137. A key factor that drives criminals and terrorists to abuse third party business structures, charities and other legal entities to transfer value is the wish for concealment of illegal assets behind an organisation's financial and economic activities. Corporate and charitable structures make it easier to obscure the beneficial owners of funds. It therefore allows the movement of funds or value while avoiding the identification of criminal individuals or entities. Often commercial structures will facilitate fictitious loans and TBML as observed in the surveillance exercise. They also provide a perceived transparency to the movement of funds, a sense of legitimacy, ensure tax efficiency and allow subsequent access to financial products.

138. The 2009 FATF Strategic Surveillance exercise builds on this, noting the following drivers (in respect of TF) relating to NPOs and charities:

- To obscure the true source of funds through the use of multiple accounts (including those of other NPOs) and transmission of funds to NPOs and individuals in conflict zones, which obscures the true purpose of the funds (see Chapter 6 for more detail on conflict zones).

- To use accounts to collect funds before transmitting them.

Enablers

139. Criminal abuse of third party business structures can take place because of the ability to use false or stolen identities to register businesses. The strategic surveillance responses have also highlighted the involvement of offshore entities (offshore jurisdictions are dealt with in Chapter 6), professional advisers (dealt with in Chapter 5) and complicit bankers as enablers. There is also the possibility of using or gaining access to third-country banks, whilst obscurity is available through complex business structures that are spread across multiple jurisdictions. Multi-jurisdictional structures of corporate entities and trusts provide further assistance in hiding true beneficial ownership.

---

22 As considered in a presentation by the IMF to the FATF Working Group on Typologies in October 2009.

140. It is difficult to verify transparency in some parts of the non-profit sector and private sector and there is often little in the way of AML/CFT controls for many of these vehicles. A general lack of awareness of the risk of abuse in parts of the charitable sector is also a contributing factor. Goodwill in respect of charities encourages donations which can then be misused by terrorist financiers. These also can operate in politically unstable areas and failed states that are attractive to terrorists.

Measures for consideration

141. In line with the conclusions reflected in the 2006 FATF typologies report on corporate vehicles, it is proposed that measures directed at this sub-feature should focus on ensuring transparency in terms of beneficial ownership.

142. A number of measures combine to reduce severity of the harms occurring as a result of the transfer of value associated with the misuse of third party business structures, charities and other legal entities (for example, those envisaged in Recommendations 33, 34 and Special Recommendation VIII).

143. The measures envisaged in Special Recommendation VIII include that countries should take steps to ensure that terrorist organisations do not pose as legitimate NPOs and that NPOs are not misused by terrorist organisations as conduits for TF or to conceal the diversion of funds collected for legitimate purposes. Further measures to address the misuse of NPOs should address all four elements of Special Recommendation VIII to include: outreach, supervision or monitoring, information gathering and investigation, and international information sharing.[23] Some countries report that they have found it useful to issue guidelines on voluntary best practice for charities.

144. NPOs can take a variety of forms, including those of legal persons and legal arrangements. Hence the measures referred to in the context of Special Recommendation VIII should be integrated with measures that provide transparency to legal persons and legal arrangements as envisaged in Recommendations 33 and 34. Implementation of these measures will provide investigative and supervisory authorities with access to information on the significant office holders of NPOs as well as third parties who may be exercising indirect control of NPOs.

145. Countries may wish to consider the risk-based approach guidance for trusts and company service providers (TCSP) issued by the FATF in June 2008.

146. Some countries have also considered establishing registries of trusts to assist investigators and the financial sector in establishing beneficial ownership. Issuing advisories to the financial sector also assists them in identifying, assessing and managing the potential risks associated with accounts maintained by shell companies.

147. Countries may also wish to implement a system to continuously screen legal persons in order to tackle misuse. The obligation to register a legal person (with certain information on the company itself and the persons who are determining the policy of the company) could be the basis for such a system. When certain circumstances concerning the legal person match the risk profile defined beforehand, the legal person concerned is designated a “high-risk legal person” whose activities will be closely monitored. This information can then be shared with the relevant authorities.

---

23 Also see: FATF (2002), *Best Practices Paper: Special Recommendation VIII (Combating the Abuse of Non-Profit Organisations)*, FATF, Paris, 11 October.

3.3.5. Retail Payment Systems and the ATM Network (including New Payment Methods)

148. Retail payment systems and the ATM network have become essential to commerce. They can be used to transfer funds electronically from person to person, to pay for goods or to get cash, anywhere in the world.

149. The importance of payment systems to commerce has spurred innovation and expansion. Barriers to accessing payment systems are falling as non-banks are increasingly offering transaction accounts that provide access to payment systems. Customers may access these accounts using cards, computers or mobile phones. For criminals and licit actors alike, payment systems have the appeal of moving value quickly, securely and cheaply. These products can help efforts to combat illicit finance by displacing cash and bringing more transactions into the regulated financial system. However, they are vulnerable to abuse because safeguards have not yet caught up with innovation and expansion.

150. In October 2006, the FATF published a typologies report on new payment methods. This report addresses the increasing role of non-banks in offering prepaid cards, electronic purses, mobile payments, internet payment services and digital precious metals. The report concluded that there is a legitimate market demand served by new payment methods and that potential ML/TF vulnerabilities exist. Specifically, offshore providers of new payment methods may pose additional ML/TF risks compared with service providers operating within a jurisdiction. In June 2008, the FATF also published a typologies report on commercial websites and internet payment systems. Abuse of new payment methods continues to be an emerging issue. For these reasons, the FATF is currently embarking on a further typology exercise on this issue.

151. The 2009 FATF Strategic Surveillance Survey noted that many jurisdictions, from a range of regions, are now routinely seeing new types of internet-based laundering or new use of new payment methods, including mobile banking, in ML activities. A limited number of jurisdictions have also cited the use of this technology for TF purposes. ML activities and the means by which proceeds of crime are generated often maximise the opportunities present in new technologies to access payment systems.

Harms

152. Use of retail payment systems and the ATM network can be enabled by use of false or stolen identities. Action by governments to lessen the negative impact of identity fraud requires significant resources and costs, which increase with the sophistication of identity fraud methods.

153. Specific harms resulting from the abuse of retail payment systems and the ATM network to transfer value by criminals and terrorists include existing and future limits placed on products as a result of abuse which may impact on innovation, business and economic development.

Drivers

154. The factors that drive criminals and terrorists to use retail payment systems and the ATM network to transfer value include the desire to avoid face-to-face transactions, to move funds quickly, securely and cost effectively and to stay one step ahead of the authorities. They also provide a location in which to receive illicit funds. Importantly they often provide prompt access from just about any place of the world. Cards which can access high-balance accounts may also be considered as a driver by permitting large value laundering, using objects of small physical size (meaning that they can easily be transported).

Enablers

155. False or stolen identities can be used to defeat CDD requirements when establishing the account. The accounts are also attractive because they can be anonymous and can be established non-face-to-face. Customer identification and periodic re-verification procedures can also be circumvented, as the account may be opened by one person but used anonymously by any other person. Furthermore, criminals or terrorists may establish multiple account relationships at multiple financial institutions, making their activity more difficult to track.

156. A further enabler is the prompt issuing of cards (some credit institutions, in order to attract new customers, send letters with cards inside, activated by a few simple operations).[24] Similarly, criminals can establish online payment system accounts instantly. This means that launderers and terrorist financiers can construct a ML/TF operation in a short space of time.

157. A key enabler relating to new payment methods is that regulation can take time to catch up to marketplace innovation. There are a great variety of electronic payment systems available. Some jurisdictions have not yet implemented appropriate safeguards for these products. As the 2006 FATF typology observed, offshore service providers may not observe the laws of other jurisdictions.

Measures for consideration

158. There is a number of wide-ranging preventive or deterrent measures contained within the FATF standards that are applicable to accounts providing access to retail payment systems and the ATM network. These measures focus on CDD, record-keeping and the reporting of unusual, suspicious or large-value transactions (*e.g.*, Recommendations 5, 9-11, 13, 19 and Special Recommendations IV and VI).

159. In relation to new payment methods, Recommendation 8 calls for financial institutions to pay special attention to threats that arise from new technologies. This is particularly true for risks associated with non-face-to-face business relationships and transactions. Measures of this nature are equally relevant for reducing the harms associated with the misuse of new payment methods.

160. One suggested measure is to make electronic payment systems a part of national AML/CFT systems (including on the legislative level). In addition, the 2006 FATF typology report sets out a range of possible measures. These include:

- Limits on the value that can be funded, stored and spent.
- Monitoring of accounts and reporting suspicious activity.
- Limits on cross-border access of funds.
- Maintaining transaction records with payer and recipient.

161. In addition, further measures might include ensuring industry/regulatory/enforcement discussion during product development so that vulnerabilities are "designed out" as far as possible. Where possible it may be useful to undertake a limited roll out of new products to test their vulnerability.

---

[24] This, in particular, is true for the countries experiencing a credit boom.

162. The FATF is currently working on a project to follow up on the October 2006 FATF typologies report on new payment methods. The 2006 report concluded that "the FATF Forty Recommendations and Nine Special Recommendations provide an appropriate framework to address the vulnerabilities associated with these new methods of payment that have been identified by the project team". Nevertheless, the 2006 report recommended that the study on the development of new payment methods as well as the typologies and risks analyses be updated after a period of two years. It is the goal of this new research project to examine if this assessment is still valid after 3-4 years of experience with such new payment methods or whether an amendment of FATF Recommendations or respective interpretative notes is necessary.

CHAPTER 4: THE ABUSE OF ASSETS/STORES OF VALUE

4.1. Introduction

163. The third feature that money launderers and terrorist financiers abuse prevalently is assets/stores of value. Crimes such as drugs and arms trafficking, theft, fraud, corruption, embezzlement of public funds, bribery and other harmful offences provide conditions for the formation of illegal capital. This is a fundamental aim of the illegal activity.

164. Criminals then seek to invest this money to provide security or profitability or hold it in a form that maintains its value. In other cases, criminals seek to store the value in ways that is otherwise convenient to them, for example, in ways that allows them to enjoy and demonstrate to others a luxury lifestyle, or allows them to easily liquidate the funds. Whatever the aim, they will seek to achieve it while minimising the chances of being caught and distancing themselves from the original activity.

165. The reported incidents of ML in respect of assets and stores of value far outweigh those relating to TF. However, that is not to say that this area is not vulnerable to both.

Assets and the global financial crisis

The crisis has seen an increase in the buying and selling of gold, an asset that some criminals consider to be attractive. Honest people have also been liquidating their financially risky investments and holding portfolios of smaller, less risky investments, including removal of capital from low capacity countries. Criminals with sums to invest are also likely to consider such investment strategies as attractive.

4.2. Major Sources of Proceeds

166. In general, all predicate offences that generate profits involve investment in assets and stores of value, including notably those associated with organised crime. In relation to financial products, in October 2009 the FATF published a typologies report on ML/TF through the securities sector. This report observed, "the securities sector is perhaps unique among industries in that it can be used both to launder illicit funds obtained elsewhere and to generate illicit funds within the industry itself through fraudulent activities". In that regard, the report also addresses three predicate offences for ML that are particular to the securities sector (*i.e.*, insider trading, market manipulation and securities-related fraud).

4.3. Overall Measures

167. In addition to the FATF requirements on confiscation, some jurisdictions have highlighted the beneficial effect of non-conviction based confiscation in attacking criminal assets because the measure can be used in a number of situations where the criminal process has either failed or is not a viable option. In such circumstances, it provides an alternative means of disrupting the lives and activities of criminals. In addition, where non-conviction based confiscation is not possible, the taxing of criminal assets can provide similar benefits.

168. In relation to managing assets recovered, countries in which asset recovery is tied to particular assets rather than to their value have reported that operating asset forfeiture custodian regimes, or asset management offices, are useful tools in preventing those assets from being dissipated. In addition, schemes

by which some of the assets confiscated are reinvested in law enforcement work can encourage further asset confiscation activity by domestic law enforcement agencies and so further boost efforts to attack criminal assets and stores of value.

169. The FATF recently issued further guidance on the above points in its best practices on confiscation (Recommendations 3 and 38) (February 2010). These best practices include having jurisdictions consider establishing specialised units or dedicated personnel with training in specialised financial investigation techniques. In addition, some jurisdictions have placed restrictions on holding certain assets by convicted criminals, which has proven to be useful when national laws allow for it.

4.4. The Sub-Features

170. The following sections consider the harms associated with abuse of the following sub-features of assets/stores of value:

- Financial products.
- Moveable goods.
- Real estate.

171. Each of the sections describes the harms specifically arising from the sub-feature, the drivers behind criminal and terrorist abuse and the enablers that allow the criminal or terrorist to take advantage of them. Finally, consideration is given to some of the measures that can be taken to allow countries to address the drivers and enablers and so reduce the harm caused. Countries may wish to consider these and other options in designing their AML/CFT strategies.

4.4.1. Financial Products (including Insurance, Investment, Saving Products, etc.)

172. The expansion of the financial services sector in recent decades means that financial products are a common means for individuals and institutions to store and increase the value they hold. There is a broad array of products available, developed in response to a wide range of customer requirements and appetites for financial risk. This expansion has been experienced in both the legitimate and criminal sectors.

173. Financial products such as securities, bonds, insurance products and savings products provide criminals with a series of opportunities for laundering illegal proceeds. Regulated financial institutions are often a guarantor of the safety of deposited money. Many of their products are strongly linked to the banking sector, either because they are provided by banks or because they are funded through bank accounts and therefore provide easy access to prompt cross-border money transfers and to a range of other products and services. Deposits held as financial products may be used as a security for loans, *i.e.*, as a security for legal funds provided to a criminal, for instance, for the purchase of real estate. In addition to that, such products generate certain profit.

174. The 2009 FATF typologies report on the securities sector established that the industry's speed in executing transactions, its global reach and its adaptability can make it attractive to criminals. Discussions

as part of the FATF Strategic Surveillance Initiative have highlighted the use of a wide range of financial products including securities transactions by organised crime as a source of funding.[25]

175. Securities trading, particularly in relation to small capitalisations can be subject to extreme price movements, and the prices of such illiquid stock may be substantially affected by relatively small transactions. The FATF securities typology observed that this mechanism has been exploited for ML purposes where block trades of illiquid stocks are transacted at a pre-agreed price between two parties. In such transactions, parties agree to the initial purchase of an illiquid security at an artificially low price with the same security being bought back some time later by the original seller or an associate at a significantly higher price. Transfer pricing of this nature is dealt with in Chapter 3, as a type of TBML.

The impact of external events on the controls applied to financial products

External events such as the global financial crisis may result in a downwards pressure on investment in AML/CFT controls in financial institutions that have been affected. Counter-pressure has been applied by work on the financial crisis by the FATF, G20 and the OECD. In some countries, government investment in financial institutions may provide greater influence which can be used to maintain or increase AML/CFT controls. Further analysis of the impact of the crisis on jurisdictions is set out in Chapter 6.

Harms

176. The abuse of financial products to invest illicit funds to launder money and finance terrorism can undermine confidence in the integrity of the financial system, damaging its reputation and that of businesses within it. Disruption of the stock market can also have a harmful effect on investor confidence and market quotations through price manipulation. Illicit investments in the markets can also strengthen organised crime groups.

177. Abuse is often enabled by identity fraud. Action by governments against identity fraud requires a significant amount of resources, which increase with the sophistication of methods of identity fraud. Widespread use of false and stolen identities could result in a lack of confidence in public sector and financial sector data-sets and processes and cause financial loss and inconvenience to natural persons that are victims of fraudulent schemes as a result of the use of illegally obtained data.

178. Extensive abuse of certain financial products can undermine social policy of increased access to the financial system as measures create barriers to individuals wishing to set up bank accounts etc.

Drivers

179. Criminal and terrorist use of financial products is driven by a need to ensure safe storage and high liquidity. Converting cash into a financial instrument allows for easy access to the funds whilst also facilitating their safe and swift movement.

180. Financial products can lend themselves to laundering in large volumes, whilst helping to confer apparent legitimacy on illicit funds by providing other business opportunities such as genuine investment in real estate or securities.

181. By purchasing large shareholdings criminals can establish and exercise control over businesses.

---

25 Presentation by the Japan Financial Intelligence Centre to the FATF Working Group on Typologies in October 2009.

Enablers

182. The complexity and international nature of the banking system allow criminals to hide illegal operations in the multitude of financial transactions carried out by financial institutions on a daily basis. The plethora of products readily available combined with a sophisticated financial environment make it possible for them to be exploited by criminals and terrorists for their own gain.

183. Businesses have a genuine and honest commercial need to maximise sales and develop attractive and competitive products. However, this can result in the focus being concentrated on business models that require quick delivery channels, favouring anonymity and are driven by commission-based remuneration packages, which criminals can take advantage of.

184. Differences in national legislations governing certain financial products and a wide variety of products available assist in making these sectors vulnerable to exploitation.

Measures for consideration

185. The most useful measures for those jurisdictions keen to attack criminally held financial products are those listed above as overall measures (Section 4.3.). These can counter the abuse of all types of assets. However because of the central role of financial institutions in issuing and trading financial products, those FATF Recommendations that directly apply to these businesses are also relevant.

186. The 2009 typologies report on securities noted that there are a number of synergies between the securities industry and other parts of the financial services industry. In particular, the report noted a trend in relying on CDD/"know-your-customer" (KYC) information gathered from the banking sector which is then relied upon in fulfilling the CDD/KYC obligations of the securities industry. The FATF is currently looking at this issue in relation to Recommendation 9.

187. Countries may wish to consider the guidance issued by the FATF in October 2009 on the risk-based approach for the life insurance sector.

188. Some countries have also identified information sharing with the financial sector, including on red-flag indicators and typologies as a useful tool to allow firms to protect themselves.

4.4.2. Moveable Goods

189. There are a range of moveable goods that are available for storing criminal funds. This includes vehicles, precious stones and gold, art, antiques and machinery. Such items tend to have a high value, therefore allowing large sums to be stored. Certain choices of asset will be less likely to attract the attention of the authorities or the private sector. Such purchases can also have the goal of gaining or maintaining a luxury lifestyle, and demonstrating this within communities. In addition, certain assets can be in themselves used for criminal purposes beyond ML, for example cars can be used to provide logistical support. Such goods also allow for the manipulation of the price of property because it can be represented as either under or over its real value, or because the value is indeterminable, for example in the case of art and antiques.

Harms

190. The investment of illegal funds in high value moveable/portable goods by criminals and terrorists allows them to enjoy the proceeds of their crime. Demonstration of the tangible benefits of a criminal lifestyle within communities can attract further individuals to crime.

191. Ownership of luxury or high value goods by criminals, which honest citizens may not be able to afford, is inequitable and so may lead to social stratification and fuel social tension. Businesses selling goods to criminals gain income not available to others; this makes complicit businesses more profitable and so creating an economic distortion.

192. Criminal activity can stimulate the development of illegal (black) markets for antiques and works of art and virtue and can result in the smuggling and moving of heritage articles out of a jurisdiction. Profits reinvested from the illegal trade in precious metals and stones into the purchase of weapons can result in the expansion of armed conflicts.

Drivers

193. Investing illicit funds in moveable goods is driven by a desire to live and maintain a luxury lifestyle. Portable goods can facilitate large-value laundering, through in some cases, objects of small physical size or the conversion of large sums of cash. Material assets which demonstrate the benefits of a criminal lifestyle can help to establish primacy in social and business groupings.

194. Converting large, questionable amounts of cash into stores of value provides criminals with permanent assets the value of which are internationally accepted (in the case of precious stones and gold). They are often able also to benefit from a return on their assets, which can then be reinvested into other criminal conduct.

Enablers

195. Criminal and terrorist investment of illegal assets in movable property is enabled by the availability of attractive goods coupled with a lack of awareness of regulations on the periphery of some parts of the regulated sector. Some goods are readily available for cash.

196. Criminals may seek to use false or stolen identities to avoid being identified by CDD requirements. By investing in other assets such as precious stones and metals, art and antiques they can leave less of an audit trail than with financial instruments.

197. The use of front men and fictitious companies (including offshore companies) when buying property, as well as the registration of properties in the names of third parties such as relatives or children can distort audit trails making the beneficial owner harder to determine.

198. The use of high value goods is compounded by the availability of international markets where this merchandise may be traded illegally. High value goods can include precious stones and metals, antiques, and works of art. Criminal use of such markets to mask their activities can lead to overpricing of works of art whose value may only have been determined hypothetically.

Measures for consideration

199. The most useful measures for those jurisdictions keen to attack criminally held moveable goods are those listed above as overall measures (Section 4.3.). These can counter abuse of all types of assets.

200. In addition, Recommendations 12, 16 and 24 extend controls to DNFBPs including dealers in precious metals and dealers in precious stones. Recommendation 20 requires for consideration to be given to extending regulation to other types of businesses and professions, which would include dealers in high value goods, if they are at risk.

4.4.3. Real Estate (Ownership and Leasing of Land and Buildings)

201. The use of real estate transactions is one of the proven and most frequent methods of ML employed by organised crime. The 2009 FATF Strategic Surveillance Survey noted that many jurisdictions consider real estate businesses to be high risk, as there are opportunities to abuse them for ML purposes. There are many ways of laundering money through real estate. For example, a real estate may be bought by a front organisation using illegal money. Profit from sale of that property can be regarded by outsiders as a legal income. Also, an unprofitable business may be purchased in order to disguise the illegal proceeds as the income generated by that business.

202. Another example is the manipulation of the price of property, so that it is represented as either under or over its real value. In the case of under-pricing, the difference is paid with "dirty" money. The real estate is then sold at a higher price. This creates an income, ostensibly earned in a legal way. In some jurisdictions illegal money is laundered through the purchase and sale of land. Illegal funds can be laundered by overstating the price of the plot of land and falsifying land appraisal documentation and purchase and sale agreements. The purchase may take place through front and fictitious companies.[26]

203. In deciding where to invest in real estate, the attractiveness of a jurisdiction will often form part of criminal decision making. For example, those jurisdictions where the climate is favourable or where others from the criminal's peer group holds property are likely to be considered as a good place to invest.

Harms

204. The characteristics of the housing market that allow abuse by money launderers and terrorist financiers also encourage mortgage fraud. The investment of illegal funds in real estate also enables criminals and terrorists to hide the beneficial ownership of property meaning that the true or full value may not be available for taxation.

205. Criminal ownership of housing, which honest citizens may not be able to afford, is inequitable. Over time this can lead to the deterioration of neighbourhoods due to criminal activity, since the ownership of housing by criminals in these areas may increase other forms of crime or illegal behaviour. Overt displays of the rewards gained from a criminal lifestyle within local communities have the potential to attract further individuals to crime.

206. Corruption of intermediaries results in the integration and acceptance of criminal behaviour into local societies. An increased criminal influence in businesses involved in real estate, can lead to distorted decision-making and formulation of professional advice, causing harm to these business sectors.

Drivers

207. Criminals and terrorists use of real estate for the investment of their illicit funds is motivated by their wish to gain or maintain a criminal or luxury lifestyle and enjoy the benefits of their illegally obtained funds. Real estate provides a permanent asset and long-term investment for criminals, which offers them the façade of financial stability and can provide security for future loans.

---

[26] Under-pricing and overpricing can also take place with companies and other non-tangible assets such as intellectual property. The laundering process is the same. They are also an important component of TBML, which is dealt with in Chapter 3.

208. The purchase of property allows large sums of illicit proceeds to be concealed and integrated. This gives the criminal the ability to obscure the true source of funds and hide the identity of the true beneficial owner amongst the large number of authentic conveyancing transactions. The ability to commingle illicit cash with a genuine income makes profits appear to be legitimate.

Enablers

209. Through investment in real estate, criminals and terrorists can look to obtain assets through the use of intermediaries, *e.g.*, real estate agents and solicitors. These individuals provide an extra layer between the criminal and the transactions he undertakes. The corruption of such intermediaries (which can include local planning officials) enables the criminal to achieve his objective more easily or further distance himself from the activity.

210. Regulatory controls can be weak in some countries, for example, there may be no restrictions or regulation applied by property registers. In these type of jurisdictions, there exists a low risk of detection; therefore, ML can be easily camouflaged among the huge number of genuine real estate transactions taking place.

Measures for consideration

211. The most useful measures for those jurisdictions keen to attack criminally held real estate are those listed under overall measures (Section 4.3.). These counter abuse of all types of assets. Countries may also wish to consider the guidance issued by the FATF in June 2008 on the risk-based approach for real estate.

212. In addition, Recommendations 12 and 16 extend controls to DNFBPs including real estate agents. Countries might also consider whether bringing leasing agents within the scope of regulation would assist in undermining criminal activity.

213. Some countries have reported benefits resulting from bringing property transfer and registration procedures under the scope of national AML/CFT regimes. For example, some jurisdictions ask their land records departments or government land offices to submit reports of large-value cash transactions and suspicious transactions to their financial intelligence units (FIUs). These reports are useful to law enforcement when investigating property that may be related to criminal activity.

CHAPTER 5: THE ABUSE OF GATEKEEPERS

5.1. Introduction

214. Gatekeepers are the fourth feature that money launderers and terrorist financiers abuse prevalently. Gatekeepers are, essentially, individuals that "protect the gates to the financial system" through which potential users of the system, including launderers, must pass in order to be successful. As a result of their status they have the ability to furnish access to the various functions that might help criminals to move or conceal their funds.

215. For the purpose of this chapter gatekeepers are considered both in the traditional sense of professionals that are able to provide financial expertise (such as lawyers, accountants, tax advisers and trust and company service providers) as well as those that have control or access to the financial system in other respects. This includes insiders, who have knowledge and understanding of the businesses within which they operate and can access financial systems and provide expertise through their position of employment. This involves the violation of the principle of confidentiality. The chapter also includes politically exposed persons (PEPs) who have access to funds and systems in their country and who may use their influence to change legislation or adapt rules for their own benefit.

216. In some cases the personal position or reputation of the gatekeeper is useful for the launderer to minimise suspicion surrounding his criminal activities, either as it lends a certain amount of credibility in the eyes of other parties because of the ethical standards presumed to be associated with such persons and professions, or because the gatekeeper's expertise allows him to undertake transactions or make arrangements in a way that otherwise avoids suspicion.

217. The reported incidents of ML in respect of gatekeepers far outweigh those relating to TF. However, that is not to say that this area is not vulnerable to both.

218. Gatekeepers will undertake either self-laundering or third-party laundering. Of the various categories, professionals tend to launder for third parties, either knowingly or unwittingly. Such individuals could in fact form part of the criminal group and may also be involved in the predicate crime. Insiders and PEPs can launder either for third parties or themselves.

5.2. Major Sources of Proceeds

219. In general, all predicate offences could be supported by laundering through the use of gatekeepers, particularly in the case of professionals. The strategic surveillance discussions have all pointed to the increased use of professionals for complex ML cases, especially those involving significant financial fraud and organised crime. Corrupt insiders also allow for the laundering of a range of predicate offences. However, it is often the case that such insiders facilitate the transfer of fraudulently obtained funds that they have generated themselves, either on their own behalf or for other criminals. PEPs similarly launder funds they have generated themselves through extracting state funds for their own benefit.

5.3. The Sub-Features

220. The following sections consider the harms associated with abuse of the following sub-features of gatekeepers:

- Professionals and insiders.
- Politically exposed persons (PEPs).

221. Each of the sections describes the harms specifically arising from the sub-feature, the drivers behind criminal and terrorist abuse and the enablers that allow the criminal or terrorist to take advantage of them. Finally, consideration is given to some of the measures that can be taken to allow countries to address the drivers and enablers and so reduce the harm caused. Countries may wish to consider these and other options in designing their AML/CFT strategies.

5.3.1. Professionals and Insiders

222. As indicated above, lawyers, notaries, accountants and other professionals offering financial advice are a common element seen in complex ML schemes. They often play a key role in helping to set up such schemes, particularly company formation agents and managers of these structures. For this reason, the FATF published a typologies report on the misuse of corporate vehicles in October 2006. The report also focussed on trust and company service providers and identified a number of frequently occurring risk factors associated with corporate vehicle misuse. The 2009 FATF Strategic Surveillance Survey also noted the increased involvement of professional advisers, including lawyers and complicit bankers, in ML schemes.

223. Professionals also manage and perform transactions in the most efficient way possible and in ways that avoid detection. In some cases, this will include real estate transactions. They also seek to conceal their activities behind "professional" status, for example, because of the reliance placed on these categories of professionals by financial institutions. This also minimises suspicion surrounding their criminal activities.[27]

224. Insiders are generally known as members of a group of limited number who have access to private, secret, privileged or restricted information. The term refers usually to the person who owns business information, but generally speaking it could apply to those in other powerful organisations such as within government.

225. The main tool insiders have is their first-hand material knowledge. They are a source of direct and useful guidance to an outsider, informing him of what really goes on behind the scenes. Therefore, potential launderers may recruit or coerce an insider into providing such services, so that they can take advantage of that knowledge.

---

27 A presentation in February 2009 by Belgium set out five types of involvement in ML/TF that professionals can provide: introduction to financial institutions, involvement in real estate transactions, performing financial transactions, establishing corporate structures/setting up legal and financial constructions and company management.

Harms

226. Abuse of professionals and insiders can damage the reputations of businesses, individuals and sectors. Professionals and insiders playing the role of gatekeepers for criminal funds can cause the integration and acceptance of criminal behaviour into local societies. This can lead to an increased criminal influence in professional businesses, which can adversely effects and distort decision making, causing reputational and financial harm to these professions and to the sectors as a whole. There also exists the potential for criminal flows to distort whole markets and prices if demand for professional services is high. This can have the follow-on effect of potentially raising prices for honest consumers. Criminals may also benefit from having access to professional services, which honest citizens or businesses may not be able to afford, thus creating an imbalance.

227. Professionals selling services to criminals gain income not available to others, making complicit businesses more profitable. Once the professional is recruited, physical and other threats may be employed to stretch the boundaries within which the complicit professional is willing to act.

228. Businesses that are exploited for ML and TF by coerced, corrupt or recruited insiders are also likely to be vulnerable to being exploited for fraud and other crimes by such insiders.

Drivers

229. When requesting the services of professionals and insiders, criminals are endeavouring to obtain expertise about how to undertake transactions, in order to successfully conceal ownership or other aspects of the transaction. Inside knowledge of a particular profession or sector can allow them to obtain financial products in an indirect or non-attributable form, making the tracing of funds or assets more lengthy and difficult. The services of professionals and insiders are often key elements to allowing criminals to circumvent preventive measures, detection and the scrutiny of the authorities.

230. In certain jurisdictions, where the intervention of a legal professional is a legal necessity to purchase real estate this will be a criminal driver, as well as a driver for legitimate use of such businesses. In addition, some criminals will seek to take advantage of professional secrecy obligations that may apply to the gatekeeper.

Enablers

231. Poor controls on information and inadequate codes of conduct and ethics with a low likelihood of disciplinary action all help to shape businesses in ways that enable criminals to take advantage of the services they offer. Professionals and insiders who are sole traders and have no management or compliance oversight, along with vulnerable business models that cannot support sophisticated AML systems, are often seen as soft targets for criminals who wish to use their services for illegal gain.

232. Professions which use sales-driven remuneration packages as motivational tools, can unwittingly promote greed or vulnerability in individuals through an absolute focus on sales and profits, if the corresponding ethics and internal controls are not present. This can offer an environment which can be readily exploited by criminals.

233. The non-disclosure and secrecy rules that apply to the relationship between gatekeepers and their clients can also prove conducive to criminals when looking to procure the services of certain professionals for criminal gain.

Measures for consideration

234. Recommendations 12 and 16 extend controls to DNFBPs including lawyers, notaries, other legal professionals, accountants and trust and company service providers in certain circumstances.

235. Countries may wish to consider the guidance issued by the FATF in October 2008 on the risk-based approach for legal professionals. Countries may also consider the similar risk-based approach guidance for accountants issued in June 2008.

236. Some countries have reported that generating publicity, sharing information and raising awareness on ML/TF threats and their associated vulnerabilities has been useful in the context of the professional sector. This can be supported by advanced tools to allow for effective monitoring of suspicious transaction reports (STRs) by FIUs to build knowledge and develop intelligence. The creation of a dedicated function responsible for receiving and analysing STRs from each profession can assist with this.

237. In addition, strong codes of conduct and codes of ethics for these professionals (supported by their supervisory and regulatory bodies) which include AML/CFT components and have corresponding disciplinary action are important. The ability for competent authorities to sanction criminal behaviour by professionals is important and the beneficial effects of this can be multiplied by publicity around such action.

238. Countries can also assess the extent to which the privilege of confidentiality in lawyer/client communication have a detrimental impact on AML/CFT effectiveness in their context and where possible take steps to mitigate this impact.

239. With respect to insiders, Recommendations 14 and 15 are important, as they strengthen the obligations and protection of the directors, officers and employees of financial institutions when reporting STRs. As well, they require the development of programmes against ML/TF which include internal policies, procedures and controls, employees training programmes and an audit function.

240. In addition, the beneficial effects of restrictions on criminals or their associates (as per Recommendation 23) or those responsible for breaches of AML/CFT controls, owning or controlling firms or otherwise being employed in the financial sector have been reported.

5.3.2. Politically Exposed Persons (PEPs)

241. Politically exposed persons (PEPs) are individuals who are or have been entrusted with prominent public functions. There is a possibility, especially in countries where corruption is widespread and applicable to the persons or companies related to them, that such individuals may abuse their public powers for their own enrichment through the receipt of bribes, embezzlement, etc.

242. Through their position, PEPs have access to significant public funds and financial arrangements such as budgets, bank accounts, publicly controlled companies and contracts. In the latter case, their gatekeeper status allows them to be able to award contracts to suppliers in return for personal financial reward. For this reason, PEPs are considered as part of the gatekeeper category. The 2009 FATF Strategic Surveillance Survey noted that PEPs are considered to be one of the largest categories of high-risk customers for ML purposes. This is consistent with how enhanced CDD should be applied to PEPs according to Recommendation 6.

Harms

243. The sums laundered through the use of PEPs are subsequently unavailable for public expenditure, increasing tax burdens or reducing services for citizens.

244. Certain PEPs, as a result of their activities, may have the ability to influence legislation or action by government authorities for their own benefit. This has the potential to inflict significant harm by undermining confidence in the actions of these institutions, including the political system itself, which can lead to increased criminality and social unrest.

245. A financial institution's reputation may be severely damaged if connected with PEPs, or it may even be exposed to increased responsibilities when accepting and managing funds from PEPs in the future.

Drivers

246. A PEP's illegal conduct is primarily driven by greed and/or a desire for increased power within the position he holds. He seeks to remove funds from public or business sectors for personal benefit. In the case of PEPs from unstable countries, they look to move their assets to another location where they will be safer.

Enablers

247. Control or ownership over domestic financial institutions, companies and government institutions and processes enable a PEP to take advantage. Variable standards and controls in the country where funds originate or the destination jurisdiction, along with high levels of corruption, and an incomplete understanding of which individuals are foreign PEPs help to create a low risk of detection.

248. It can also be difficult for authorities to scrutinise and investigate PEPs. For example, in many countries investigators need particularly strong evidence if a search warrant application relates to a PEP. In the case of diplomats, the authorities of the country in which such individuals are accredited have limited ability to question, search or investigate persons having such status.

Measures for consideration

249. Recommendation 1 requires countries to apply the crime of ML to the "widest range" of predicate offences. Ensuring that this includes corruption and bribery is important to attacking the harms caused by PEPs. Application of Recommendation 3 on confiscation is effective, as it attacks the main driver of PEPs – the acquisition of funds. Also effective are measures relating to international co-operation on asset recovery (Recommendation 38) and mutual legal assistance and extradition(Recommendations 36 and 39). Recommendation 6 is also a key measure as it requires enhanced due diligence in relation to PEPs.

250. Recommendation 13 obliges financial institutions to report financial transactions of funds suspected to be the proceeds of criminal activity, including bribery and corruption. Recommendation 16 extends this obligation to DNFBPs. Financial institutions are required to put in place adequate procedures to screen prospective employees to ensure high standards (Recommendation 15). This obligation also applies to DNFBPs (Recommendation 16). When applied effectively, these measures would prevent a prospective employee from being hired by a financial institution when a conviction for corruption or bribery has been detected. Similar measures are contained in the FATF standards to prevent a prospective employee with a possible criminal background from being hired by a financial institution (Recommendation 23) or by a casino (Recommendation 24).

251. The issue of how to address corruption is also addressed in the context of Recommendation 26 on FIUs. An FIU must have "sufficient operational independence and autonomy to ensure that it is free from undue influence or interference." For example, an FIU might be prone to by undue influence by more powerful (and corrupt) officials rendering it open to charges of abuse of function. Related to this is Recommendation 30 which calls for government agencies involved in AML/CFT to ensure that financial sector supervisors, prosecutors and investigators are of high integrity.

252. In addition, ratifying and implementing relevant international conventions against corruption (*e.g.,* the *United Nations Convention against Corruption* [UNCAC], the *OECD Convention against Bribery of Foreign Officials*, the *Inter-American Convention against Corruption*, etc.) is an important starting point.

253. Some countries have reported lifting the immunity from criminal prosecution for heads of state, government officials and political figures as a useful measure. Operationally, referring large transactions to host countries can prevent funds being removed by PEPs, and the creation of an independent, dedicated anti-corruption body and asset registries for public sector officials can also be beneficial as can the introduction of financial disclosure requirements for PEPs.

254. Widening the definition of PEPs to include domestic PEPs enhances the scrutiny applied to such persons and therefore can limit their ability to remove funds from the jurisdiction. Although there is no obligation under the FATF standards to provide for enhanced due diligence of domestic PEPs, the FATF Interpretive Note to Recommendation 6 encourages countries to extend the requirements of the Recommendation to individuals who hold prominent public functions in their own country. At the same time it is important that the inclusion of the risk based approach in Recommendation 6 is considered to make it a more focused and effective tool for identifying high risk individuals and PEPs.

CHAPTER 6: THE ABUSE OF ENVIRONMENTAL / JURISDICTIONAL ASPECTS

6.1. Introduction

255. The fifth and last feature that money launderers and terrorist financiers abuse prevalently relates to environmental and jurisdictional aspects. ML and TF continue to be predominantly cross-border activities.[28] Because a chain is only as strong as its weakest link, the international community must rely on all countries to establish effective AML/CFT regimes that are capable of successfully preventing, detecting, prosecuting and imposing sanctions on ML/TF in order to counter the negative consequences of these criminal activities. In effect, the harms that flow from having a weak AML/CFT regime in one jurisdiction may have negative consequences beyond its own borders.

256. There is no universally agreed definition as to what represents a high risk of ML/TF for a particular country or geographic area. In fact, ML/TF activity can occur anywhere in the world. However, certain countries are more likely to attract these illegal activities. Certain jurisdiction-specific aspects attract criminals and terrorists who always seek to work in a friendly environment where the risk of detection is relatively low. Other aspects such as a sound financial sector will appeal to criminals that want to safeguard their funds or appear to be legitimate. Criminals and terrorists will target the jurisdictions and institutions that suit them best.

257. It should also be observed that there will always be an environmental or jurisdictional aspect to successful ML/TF, as the activity always needs to take place somewhere. While much ML/TF is global, often involving two or more jurisdictions, for many criminals, particularly low-end domestic criminals, there will be no choice to make. They will have no option but to launder their proceeds in the country where they live or operate. In the case of TF, the funds will need to reach the particular location where the terrorist or organisation can make use of them or where the terrorist activity is to take place.

6.2. Major Sources of Proceeds

258. Given the broad, overarching nature of this feature, environmental and jurisdictional aspects will feature in all ML and TF in one way or another. The 2009 FATF Strategic Surveillance Survey noted that the most commonly cited risk factor – geographic location – mirrors the factor identified with respect to the customers themselves. A number of respondents noted that the involvement in a transaction of any geographic location of concern for terrorism raised a red flag for them. The identification of groups involved in terrorist activities, violent criminal activity and drug trafficking/production has resulted in frontiers and cocaine production areas now being considered high-risk areas for TF as well as for narcotics trafficking.

6.3. Overall Existing Measures

259. Full implementation of FATF measures is relevant to reducing the negative impact of environmental and jurisdictional aspects. This is because the failure to implement some or all of the FATF

[28] As confirmed in the 2009 FATF Strategic Surveillance Survey.

Recommendations in a particular country weakens not only its AML/CFT regime but also global AML/CFT efforts more generally. For this purpose, measures can be considered as falling within two categories.

- The first category covers the measures that the country itself may take to advance the fight against ML/TF. This consists of implementing the bulk of the FATF Recommendations and other guidance.

- The second category covers the countermeasures that the international community may take in respect of countries having deficiencies in their AML/CFT standards. These relate primarily to Recommendation 21, which requires financial institutions to give special attention to countries that do not sufficiently apply the FATF standards, and its implementation by FATF members. Recommendation 21 also allows countries to apply appropriate countermeasures to those countries that do not apply or insufficiently apply the FATF Recommendations.[29]

260. In addition, the international community may address this issue by lending assistance to such countries, for example technical advice and capacity building efforts.

6.4. The Sub-Features

261. The following sections consider the harms associated with the abuse of the following sub-features of environmental / jurisdictional aspects:

- Variable standards and controls.

- Major financial centres, tax havens & offshore banking centres.

- High-risk and conflict zones (*e.g.*, areas known to have a concentration of terrorist or criminal activity).

- Jurisdictions with high levels of corruption.

---

[29] Examples of possible countermeasures include:

- Stringent requirements for identifying clients and enhancement of advisories (including jurisdiction-specific financial advisories) to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from these countries.
- Enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious.
- In considering requests for approving the establishment in countries applying the countermeasure of subsidiaries or branches or representative offices of financial institutions, taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems.
- Warning non-financial sector businesses that transactions with natural or legal persons within that country might run the risk of ML.
- Limiting business relationships or financial transactions with the identified country or persons in that country.

262. Each of the sections describes the harms specifically arising from the sub-feature, the drivers behind criminal and terrorist abuse and the enablers that allow the criminal or terrorist to take advantage of them. Finally, consideration is given to some of the measures that can be taken to allow countries to address the drivers and enablers and so reduce the harm caused. Countries may wish to consider these and other options in designing their AML/CFT strategies.

6.4.1. Variable Standards and Controls

263. ML and TF are global problems that need to be fought collectively by the international community. The strength of the global AML/CFT measures depends on the strength of its weakest link. The lack of adequate systems of control due to varying standards and controls across some jurisdictions can be a weak link in the global fight against ML/TF.

264. The international community expects that all jurisdictions should have comprehensive legal, regulatory and operational frameworks to lessen the severity of their ML/TF risks. Jurisdictions that do not have such frameworks expose others to risk by failing to implement effective frameworks. For this reason the FATF has agreed that, when a country chooses not to engage in the fight against ML/TF in a meaningful way, the FATF must be ready to take firm action.[30] The 2009 FATF Strategic Surveillance Survey also identified jurisdictions which lack adequate AML/CFT systems as posing a significant risk.

Harms

265. Specific harms resulting from the existence of variable standards and controls in a jurisdiction can result in a reduction of the effect of other AML/CFT measures in other jurisdictions and in the inability of a jurisdiction to co-operate in AML/CFT matters regionally and internationally.

266. Those jurisdictions with weak controls are likely to be subject to the integration, acceptance or influence of criminal behaviour in their jurisdictions. Subsequent negative reactions from the international community such as bi-lateral or multi-lateral economic or other measures can cause socio-economic difficulties for the population. These measures may also hinder the jurisdiction's ability to access the international financial system and conduct international commerce. Moreover, any countermeasures taken by the international community may ultimately lead to reduced governmental assistance and foreign direct investments into the local economy.

267. A lack of political will to empower AML/CFT institutions and enforce applicable laws can also drive criminals into an alliance with the political elites. In addition, to the extent that a country is viewed as a haven for ML, it is likely to attract further criminal activity.

Drivers

268. The main reason criminals and terrorists take advantage of a jurisdiction with variable standards and controls is to avoid detection. Detection is more likely in jurisdictions with stronger controls.

Enablers

269. There is a wide range of enabling factors for such abuse, which primarily stems from the existence of weak or inappropriate standards and controls. These include:

---

30 As confirmed in a speech by the FATF President Paul Vlaanderen at the MONEYVAL Plenary on 23 September 2009.

- A low level of political support, resource constraints and effectiveness/cooperation of authorities.

- The absence of a comprehensive enabling law which creates a feeling of impunity and empowers criminals to take advantage of the system. It weakens the regulatory and enforcement entities and exposes the personnel of these entities to unmitigated corruption.

- Low capacity countries (LCCs): some jurisdictions have very low capacity to implement comprehensive AML/CFT measures regardless of the political will and the adequacy and efficacy of their laws.

- External events such as the financial crisis may act as a further enabler, as it may further inhibit political support and the resources available for AML/CFT. In the case of LCCs, capacity may be further inhibited as government spending is directed to areas considered more essential, and in non-LCCs there will be pressure on governments not to impose further burdens on business that that may be beneficial for AML/CFT purposes.

Measures for consideration

270. As described above, all FATF measures are relevant to addressing the weaknesses of jurisdictions with variable standards and controls. The relative importance of each will depend on the context. The countermeasures contained within Recommendation 21 are supported by the mutual evaluation process, which identifies strengths and weaknesses and makes practical recommendations on how best to remedy shortcomings. Technical and financial assistance and capacity building provide ways in which other countries can help those with weaknesses address them in a targeted and prioritised manner. In many LCCs for example, cash transactions as part of total economic activity are very important. Strengthening financial inclusion in those countries is then very important for reducing the seriousness of these risks.

271. In addition, denying banking licenses to foreign banks that do not have adequate AML/CFT systems, as well as more generally denying the access of criminals to their financial sector, has been identified by some jurisdictions as a useful measure.

Environmental and jurisdictional aspects and the global financial and economic crisis

The global financial and economic crisis has affected most of the countries in the world, undermining the stability of financial systems, with direct consequences on societies and the global economy. The crisis has highlighted the consequences of globalisation, and the interconnectivity of national markets. It has emerged that the global search for stability and robustness of the financial system depends on the integrity of the systems of the individual jurisdictions. The FATF is aware that the need for stability underlines the importance of efforts against ML /TF. Subsequently, there is a need to:

- Identify and engage with high risk and uncooperative jurisdictions.
- Achieve a higher level of compliance with the FATF standards globally.
- Create a higher level of transparency in national financial systems.

6.4.2. Cash-Intensive Economies

272. In cash-intensive economies, illegal money can easily be integrated into the national economy. In such economies, large cash transactions may be very common, as individuals are more likely to conduct transactions in cash and carry a lot of cash around with them. In some countries, this is mainly due to ethnic, cultural and historical factors that predate the spread of western banking systems in the 20th century.

273. This environment can make it difficult to prevent and detect ML/TF activities that are cash-based. However, since not all underlying crimes generate cash proceeds, there are limits to the useful mechanisms and thus the general attractiveness that cash-intensive economies may present to money launderers and terrorist financiers.

Harms

274. The abuse of cash-intensive economies by criminals and terrorists results in the removal of liquidity from the formal financial sector in the country where the criminal activity takes place. Funds that would otherwise remain in a particular country are instead moved to cash-intensive economies and invested in assets, for example property. This can be seen as a distortion of financial flows and investment in economies for non-market reasons.

Drivers

275. The main factor that drives criminals and terrorists to use cash-intensive economies is the desire to obtain, hold and move cash without attracting attention, to prevent detection and to distance the criminal from the crime, since cash – in a cash-intensive economy – is ubiquitous. Cash is easily acceptable and can be interchanged with most goods and services. It can be used for value transformation which further distances the criminal from the crime. Finally, criminals and terrorists wish to finance other crimes whilst avoiding detection.

Enablers

276. Criminal and terrorist use of cash-intensive economies is enabled by the non-monitoring of cash transactions and lack of limitations on the amount of cash that can be exchanged for goods and services or the non-observance/enforcement of such limitations. Such jurisdictions also provide an opportunity for mingling cash derived from criminal activity or terrorist funds with legitimate cash.

277. Cash-intensive economies allow for cash to be placed into an entry point that will then allow value to be moved within the global financial system and for cash to be transformed into other assets (which in turn is enabled by the presence of gatekeepers willing to facilitate such transactions – see Chapter 5 for more details on gatekeepers).

278. Such jurisdictions also provide facilities for exchanging currency, or provide access to goods and services through multiple currencies

Measures for consideration

279. Cash-intensive economies have reported that steps by the government to provide cheap and accessible banking services to the unbanked are possible and useful. Customer identification requirements for cash deposits and/or withdrawals may also provide an extra control at the point where the cash and the non-cash economies intersect. This may be challenging to implement but potentially beneficial.

280. Measures described in Chapter 2 may also be relevant to addressing any harm caused by cash-intensive economies. One particular challenge for cash-intensive economies is to establish appropriate and rational thresholds with respect to AML/CFT reporting requirements for large-value cash transactions and cross-border movements of cash. With respect to the latter, it should be noted that a basic principle is that measures should be implemented in such a way that legitimate activities are not unreasonably hindered or obstructed. In addition financial inclusion, particularly in cash-intensive economies, should be stimulated since increased financial inclusion helps to reduce the risks related to cash.

6.4.3. Major Financial Centres, Tax Havens & Offshore Banking Centres

281. Major financial centres have been identified as a magnet for the laundering of funds generated from a variety of illicit activities. In these jurisdictions, a large number of financial institutions frequently engage in international business transactions involving significant amounts of money making it difficult to identify or to detect unusual or suspicious operations. In some cases, major financial centres include geographically small jurisdictions that have a significant financial sector. While the level of criminal activity within these jurisdictions may be limited, these centres are often attractive venues for criminals to place, hide or disguise criminal proceeds earned in a different jurisdiction.

282. Tax havens and offshore banking centres are a specialist application of financial centres. These jurisdictions are characterised by financial activities with non-residents in numbers or volumes that are disproportionate to the size of their real economies. The 2009 FATF Strategic Surveillance Survey highlighted that offshore jurisdictions (particularly those with favourable tax systems) are an important risk factor. Some of these jurisdictions have also been associated with excessive bank secrecy laws, which mean that financial information requested from governments abroad might be rejected.

The global financial crisis and transparency

The crisis has increased the pressure on some jurisdictions to increase transparency. In some cases changes in transaction patterns have been observed. For example, funds are withdrawn and returned to home countries due to concerns over the security of banks or because of increased international co-operation.

Harms

283. The abuse of major financial centres, tax havens and offshore banking centres by criminals and terrorists can cause reputational damage to jurisdictions whose vulnerabilities have been exploited. It can also cause the removal of liquidity from other jurisdictions and result in financial flows and investment in economies for reasons that are not driven by the supply and demand of legitimate markets.

284. Such abuse can also result in the integration, acceptance or influence of criminal behaviour in jurisdictions. As with the abuse of other environmental or jurisdictional features, it can reduce the effect of other AML/CFT measures and transparency in other jurisdictions. In the case of tax havens, movement of criminal funds to these areas makes them more difficult to detect and reduces the application of taxes to them.

Drivers

285. The factors that drive criminals and terrorists to use major financial centres, tax havens and offshore banking centres include the wish to hold funds in a secured and regulated environment. Criminals and terrorists also need to put their funds in locations with sufficient capacity to store and process them. Such jurisdictions can also provide easy connectivity with other jurisdictions and access to a wide range of products and services thus providing further benefits.

286. Criminals and terrorists may also wish to appear legitimate by participating in regulated markets. In the case of tax havens criminals wish to avoid loss of laundered proceeds due to taxation.

Enablers

287. Criminal and terrorist use of major financial centres, tax havens and offshore banking centres is enabled by the large volumes of legal transactions that take place in these locations which make it difficult

to spot illegal transactions. In such an environment, it is difficult to distinguish legitimate from illegitimate sources.

288. A lack of transparency or excessive secrecy laws, for example on beneficial ownership, reduces visibility as do limitations on international co-operation.

289. The ease of setting up legal structures means that the time and effort of establishing ML/TF schemes is reduced. Such locations also allow easy access to other intermediaries willing to conduct the transactions in these centres on behalf of criminals or terrorists.

Measures for consideration

290. For major financial centres, all FATF Recommendations are relevant. Because of the central role of financial institutions in these jurisdictions, those Recommendations that directly apply to these businesses are relevant. As noted above, according to Recommendation 4 countries should ensure that financial secrecy laws do not inhibit the implementation of the FATF standards. Also, law enforcement and competent authorities should be able to obtain documents and information, including financial institution records, when conducting investigations of ML, TF or the underlining predicate offense as called for in Recommendation 28. The authority for financial regulators to compel the production of information from financial institutions when conducting examinations is also called for in Recommendation 29.

291. For tax havens and offshore banking centres, Recommendation 18 which prohibits shell banks and banking relationships with such entities is important. Requiring that banks maintain a physical presence in the jurisdiction where they are licensed and supervised, including the "mind and management" of the bank may also help.

292. The aspects of Recommendation 5 which relate to the identification of beneficial ownership are also important, along with any further measures to promote greater transparency for products/services such as abolishing any excessive secrecy provisions which do not allow competent authorities to determine the true beneficial owner.

293. International co-operation is also important, including on criminal matters and mutual legal assistance as called for in Recommendations 36-40. In particular, countries should not invoke financial institution secrecy or confidentiality laws as a ground for refusing to provide co-operation.

6.4.4. High-Risk and Conflict Zones (i.e., areas known to have a concentration of terrorist or criminal activity)

294. Countries that are subject to severe political, social or economic upheaval often also suffer significantly from crime and terrorism as well as ML/TF. This criminal and terrorist activity may be as a result of the upheaval; however, at times this activity may also be a contributing factor to the upheaval itself. Such countries can be those that are subject to sanctions, embargoes or similar countermeasures; those with significant deficiencies in their AML/CFT laws and regulations; those having significant levels of corruption or those countries with criminal or terrorist activities.

295. The 2009 FATF Strategic Surveillance Survey showed that, for many countries, the existence of major criminal/terrorist activities in certain locations represents an indicator of ML/TF.

Harms

296. The abuse of high-risk or conflict zones by money launderers and terrorist financiers can cause possible injury and death in such jurisdictions, as their activities can promote or inflict further violence or other dangerous activity by criminals and terrorists.

297. Criminal activity in these jurisdictions also causes reputational damage and could result in the application of international sanctions, causing harm to governments and social institutions. The existence of TF or ML activity can also hinder legitimate efforts to provide charitable or humanitarian assistance in these regions.

Drivers

298. The main factor that drives criminals and terrorists to use high-risk or conflict zones is the need to place or move money where it is needed in order to finance terrorist or criminal activity. Such jurisdictions represent a secure environment where criminal activity may not be detected or addressed by the authorities due to the prevalence of conflict or other problems. In fact, criminal activity may even be used to as a means to drive and sustain the conflict.

Enablers

299. Criminal and terrorist use of high-risk or conflict zones is enabled by a number of factors. Political and social upheaval in these areas allows for transactions and criminal activity to be hidden from view. Such conditions can allow for other forms of support to be co-located in the same geographic areas.

300. The international community's attention may not be focused on the jurisdiction if it is not considered economically and politically significant. This along with an environment under conflict where corruption is likely to be more readily tolerated can enable criminal activity to go on unchecked.

Measures for consideration

301. Regulation and supervision of money transfer businesses and alternative remittance services are important in this context, in line with Special Recommendation VI, as many high risk and conflict zones are serviced by such businesses. In addition, physical cash movements and NPOs often serve as complementary financial channels for these zones, making Special Recommendations IX and VIII important (see Chapters 2 and 3 for details). With respect to NPOs, countries should develop and promote measures that minimise risk including guidance to the donor communities and charitable sector on risk factors, risk mitigation practices and role of government.

6.4.5. Jurisdictions with High Levels of Corruption

302. Corruption and ML often occur together, with the presence of one reinforcing the other. Thus corruption facilitates ML and vice versa. Corrupt persons need to undertake ML in order to realise a profit from their corruption.

303. In addition, ML can be carried out with reduced risk if public officials can be persuaded to co-operate. Thus the bribing of PEPs becomes a key part of the conduct of the illegal activity. The presence of PEPs in a jurisdiction means that it suffers and/or poses a ML risk.[31]

---

[31] A PEP may also be considered as a gatekeeper in accordance with Chapter 5.

Harms

304. Laundering allows corrupted persons to move and realise a profit from their corruption and embezzlement. Where such laundering allows for bribery in public procurement, this undermines trust in governments and institutions. The subsequent unavailability of the laundered funds for public expenditure can result in increasing tax burdens or a reduction in services for citizens.

305. In addition, there is a strong correlation between good governance and corruption. The higher the level of corruption in a jurisdiction the more likely it is to have a lower good governance index.

Drivers

306. The main factor that drives criminals and terrorists to use jurisdictions with high levels of corruption is the need to extract and move funds away from these jurisdictions. Alternatively, the driver may be to utilise corrupt persons to assist with the laundering of criminal proceeds from other jurisdictions.

Enablers

307. Criminals and terrorists take advantage of the absence of effective and sufficiently independent government regulatory, enforcement and prosecutorial institutions to enable them to exploit corrupt persons to support their criminal activity.

308. The control or ownership of domestic financial institutions, companies and government institutions and processes by corrupt persons helps to provide an environment in which their activities can thrive. This can include the infiltration of investigative and judicial bodies or through ensuring their immunity from prosecution or extradition.

309. A long history or high levels of corruption together with a culture or tolerance of bribery creates a low risk of detection where laundering is concerned. Poor standards and controls including ineffective rules on public procurement, along with low pay and poor conditions for those in the public sector can make these areas particularly vulnerable to corruption.

Measures for consideration

310. Those measures listed to address PEPs as gatekeepers are relevant here. See Chapter 5 for further information.

311. In addition, as mentioned in the introduction to the FATF 2004 Methodology for Evaluations, jurisdictions should also respect principles of transparency and good governance, and participate in regional or international anti-corruption initiatives and commit themselves to implementing international legal frameworks such as the *United Nations Convention against Corruption*.

312. The FATF plans to conduct further work on corruption, including with a focus on Recommendation 6 (PEPs) and Recommendation 26 (FIUs). The FATF will undertake the work on Recommendation 26 in the context of the work which it has already started on operational issues (Recommendations 27 and 28).

CHAPTER 7: CONCLUSION

313. This chapter first describes the process used to produce the GTA, summarising the main systemic threats identified in it, and inviting FATF and jurisdictions to use the GTA and national ML/TF assessments to design and implement measures to address threats identified. It then suggests some next steps, including that more effort should be made to produce national ML/TF assessments.

314. Combating ML/TF requires an ongoing understanding of the methods used by criminals to launder their illicit funds and terrorists to fuel terrorism. These methods range from well-known practices established over many years to modern techniques that exploit innovations in global payment networks and continuous advances in technology.

315. The GTA has identified the systemic ML/TF threats through the analysis of typologies studies, mutual evaluation reports and the results of the FATF Strategic Surveillance Surveys. These threats identified the use of cash, internet-based systems and new payment methods, complicated commercial structures and trusts, wire transfers, and trade-based transactions, often involving the use of false or stolen identifies. Threats in this area continue to be global in nature, often involving two or more jurisdictions. They are carried out using both formal and informal systems, as well as multiple sectors and techniques. However, it is not possible to be more specific than this due to a lack of factual, reliable and quantifiable data.

316. This report has also provided a global view of the main systemic criminal and terrorist threats involving finances by providing a new way of thinking about how and why those threats manifest themselves. It has identified the key features abused by criminals and terrorists to carry out ML/TF activity and for the first time described the various harms caused by such activities along with why governments and international bodies should be concerned. It has as well established the reasons why criminals and terrorists abuse particular sectors, products, methods, and mechanisms and in the process identified vulnerabilities. In addition, the GTA has indicated examples of practical measures that can be considered to reduce the severity of the ML/TF threats which have been identified.

317. How these concepts might apply will vary from country-to-country. Some of the harms may apply globally, while others will be country specific, and there may be some additional harms that are not captured in this assessment. Countries should be aware of the harms that are relevant to them and should thus target ML/TF activity that causes them.

318. The measures that are available to address ML/TF threats will likewise vary from country to country, and those described here do not represent an exhaustive list of every available action. Rather, they give an indication of the areas that a country may wish to consider in countering specific ML/TF problems. Additionally, countries are likely to have their own, adapted measures, which should also be further developed and implemented in response to the problems they face.

319. All countries must deal with the challenge of allocating scarce resources to fund AML/CFT programmes and other public policy and safety efforts. In the budgeting process, it is important to identify and prioritise issues that require the most immediate attention. This process requires an understanding of the ML/TF threats and associated vulnerabilities relevant especially to the country's economy and financial institutions. It is hoped that this report will provide a tool that can help governments make

decisions about how to best utilise resources and set priorities for regulatory institutions and the criminal justice system.

Next Steps

320. To date, few countries have conducted a national assessment of their ML/TF risks, threats or vulnerabilities. The FATF is in the process of developing international best practices to assist in conducting assessments at the national level. Therefore, the FATF encourages all jurisdictions to conduct their own national ML/TF assessments. Such assessments will assist jurisdictions in implementing the FATF standards in a logical fashion based on risk, and will also assist FATF's future efforts to carry out similar assessments at the global level. Countries are encouraged to use the GTA framework described in Annex C as a tool when conducting their own national assessments. The FATF could consider introducing an explicit requirement for national assessments which would help governments effectively implement their AML/CFT regime and allocate resources accordingly.

321. In addition, countries are encouraged to use this GTA and their own national assessments as a basis for joint public/private sector dialogue.

322. The FATF has been charged with the role of determining responses to emerging threats in a timely manner. Experience has demonstrated that the collection and assessment of reliable and quantitative data on current ML/TF threats on which to base these determinations is difficult. Efforts to improve the amount and quality of data would be a welcome development in order to gain a better understanding of the threats. The FATF could consider introducing more stringent requirements about what data on crime, proceeds of crime and ML/TF that jurisdictions should collect, collate and publish.

323. As mentioned in Chapters 2 through 6 and in the conclusions above, the abuse of many of the features is facilitated through the use of false or stolen identities. The use of false or stolen identities has the potential to undermine all of the preventive measures in the FATF Recommendations, as they are based on the logic that users of the financial system present credible identification documents. There is no FATF measure that specifically addresses how to combat the use of false or stolen identities in the financial system. The FATF could consider doing more work to identify potential measures and to share best practices.

324. The FATF will continue to examine and produce typologies studies which provide detailed information about the ML/TF methods, trends and techniques. As more countries produce their own assessments, it should become easier for the FATF to identify the key global systemic threats with more precision.

325. The FATF's policy-making process is encouraged to use the GTA framework when prioritising and determining which ML/TF threats and associated vulnerabilities require further study, attention and better understanding. The FATF is also encouraged to consider the table of measures contained in Annex D.

ANNEX A: THE GTA FRAMEWORK

The GTA uses a tailor-made framework which sets out:

- **The *features* that are abused by money launderers and terrorist financiers.**

  To help build understanding of the specific harms of various ML/TF activities, they have been broken down into their key constituent features. These features are the building blocks of ML/TF, as almost all ML/TF activity must make use of one or more of these features.

  The listing of the features in this GTA is not intended to set out all ML or TF methods, but rather to help identify the key distinguishing factors in the process. These features in themselves may not pose a stand-alone ML or TF threat. The threat arises when the appropriate safeguards are not in place or adhered to thus allowing money launderers or terrorist financiers to abuse them.

- **The main *harms* that are caused by the abuse of these features.**

  The GTA looks at the impact and effect of abuse of the features by money launderers and terrorist financiers to carry out ML and/or TF. ML and TF are harmful – they have a negative impact or effect on individuals, communities, societies and economies, and there are also various types of harm – physical, social, environmental, economic, and structural. Harms are the underlying consequence of a threat if left unchecked. It is because of these harms that the authorities attempt to tackle ML/TF.

- **The *drivers* and *enablers* (or reasons for use) that attract criminals and terrorists to these features and allow them to be abused.**

  The primary reasons why money launderers and terrorist financiers use the features fall into two groups:

  - *Drivers* refers to the goal that the criminal or terrorist is trying to achieve.
  - *Enablers* refers to aspects of the feature that allows the criminal and terrorist to abuse the feature to achieve their own ends.

- **How the harms can be reduced or mitigated through the application of various *measures.***

  These are actions which can be taken at a local, national, regional or global level in order to make it more difficult for money launderers and terrorist financiers to use the features to conduct their criminal activities. Ultimately, these actions seek to reduce the harms caused to individuals, communities, societies and economies.

  At the national level, these measures cover the legal and regulatory framework (including the criminal justice and law enforcement system) and the preventive measures to be considered by the financial sector and other relevant professions. They include the FATF Recommendations which are designed to assist national jurisdictions in developing and enhancing AML/CFT provisions related to the judicial, regulatory and institutional systems and the implementation thereof.

  ML and TF methods and techniques will change in response to new measures being developed by individual jurisdictions or international standard setters such as the FATF.

ANNEX B: PRACTICAL APPLICATIONS OF THE GTA AND ITS FRAMEWORK

Users can draw upon the content of the GTA and are also encouraged to develop their own report in line with their specific requirements. For example, the GTA is likely to accurately reflect the nature of ML/TF in many individual jurisdictions; however, each jurisdiction can develop this content by tailoring it to specific sub-features, drivers, enablers, resulting harms identified in that jurisdiction and then develop the most appropriate measures for that jurisdiction. The resulting tailored detail will vary from jurisdiction to jurisdiction.

Below are some examples of the many practical applications of the GTA and its framework:

(1) For Authorities conducting Geographic Assessments:

At national level: The use of the GTA in order to create a national assessment is the most obvious example and is referred to several times within the GTA. Other FATF documents also make reference to this application (*e.g.*, FATF work on national threat assessments).

At regional level: The same approach can be made at a regional level. For example, two or more jurisdictions might be linked by geography, financial or trade routes or criminal group associations. A regional level approach to the assessment could therefore focus on specific features or sub-features which may be relevant to a particular region (*e.g.*, cash movements and smuggling).

At local level: There is extensive potential to use the GTA to build knowledge and create AML/CTF plans at local levels. The example box below illustrates how one FATF jurisdiction has successfully used this approach to address significant national scale ML by individuals and businesses in a small district within one city.

A number of law enforcement agencies worked together with the relevant financial supervisors, the regulated sector, professional associations and community leaders in order to identify the *features* and *sub-features* (in this case they were cash placement, transfer of value and gatekeepers).

Following this, the *drivers* and *enablers* for successful laundering were also identified (in this case the latter included social and ethnic relationships).

The *harms* were identified and this was found to be useful in winning support from community representatives who could articulate to the community that the presence and actions of the authorities were to alleviate the social and economic harms brought about by widespread ML. Here, GTA also played a role in developing a public media strategy to raise awareness and to gain public support for AML/CTF.

Finally, a range of *measures* (or actions[32]) were agreed. This included investigation and prosecution by law enforcement, increased supervision by regulators and communications by community leaders.

[32] It can be seen that the use of the term *measures* does not necessarily require legislative steps or changes to international standards but includes any potential action that can deter or detect ML/TF activity.

(2) For Law Enforcement operations against organised crime groups (OCGs):

The GTA can be an effective tool in developing a strategy to reduce the effectiveness of an OCG by undermining its ability to finance its criminal business and retain its profits. Such an approach complements a wider strategy to dismantle the OCG through all available lawful means. Similar to the example noted above, these strategies could look at the particular *features* or *sub-features* that a specific OCG may be exploiting. These strategies should aim at utilising existing law enforcement authorities and functions in a targeted approach to maximise results and effectiveness.

Law enforcement specialists are accustomed to identifying the criminal *drivers* – as knowing a criminal's motives identifies his vulnerabilities and leads to the identification of effective *measures*.

For example, criminal A may be motivated by the enjoyment of overt wealth as opposed to criminal B who seeks low visibility long term financial security and criminal C who wants the power and influence that wealth can bring. The actions to undermine those drivers will differ between criminal A, B, and C.

Similarly, the factors that *enable* this particular OCG to launder successfully will be different and so tailor-made *measures* will be needed in order to prevent or to detect such activity.

It is likely that the *harms* caused by a particular OCG will be well known. However the added value of applying the GTA framework in these circumstances is when it is applied to a number of OCGs to enable resource decisions to be made about priorities (relative degree of harm, likelihood of the successful application of measures etc).

(3) For Financial Sectors:

The GTA can be used as the basis for joint public/private sector dialogue.

Representatives from the private sectors that might provide information on a particular *feature* or *sub-feature* can join with their regulator, law enforcement agency and policy makers in order to deepen joint understanding of the feature, the reasons for its successful misuse by criminals (*drivers* and *enablers*), the resulting *harms* and the potential *measures*.

This should lead to improved exchange of information, increased shared knowledge and appropriate proportionate responses to ML/TF threats. This dialogue can also serve as a valuable mechanism to exchange feedback between the public and private sectors.

(4) For Policy Makers:

Government policy makers can draw upon the evidence produced by the above applications of the GTA in order to review the effectiveness of their own national AML/CTF regime. For example, the GTA can be used to establish whether there are many resources and measures in some vulnerable areas and too few (or none) in others .This can assist the decision-making process in relation to whether laws and regulations are proportionately applied to the areas of most concern and about which measures are effective and appropriate.

The GTA is also an effective vehicle for policy makers to influence stakeholders (e.g. politicians, law enforcement, regulated sector) and interested parties (e.g. media, the public) that the indirect harms of ML/TF are real and worthy of continued attention. The GTA is extremely useful in obtaining the necessary political level commitment to strengthen AML/CFT legal and regulatory frameworks. The use of the GTA

could be a useful mechanism to brief legislators on the need to strengthen and update laws to ensure that their address current threats.

(5) For the FATF Working Group on Typologies (WGTYP):

Shared learning from the above uses of the GTA will enable the FATF to deepen its understanding of systemic ML/TF threats and any identified associated vulnerabilities that may require further study by the WGTYP. This will lead to an ever improving global picture for future iterations of the GTA.

Future FATF typologies studies: could be produced using the GTA framework, namely:

- A description of the typology/*feature* (*i.e.*, how it works in the real world).
- what *drives* criminals to misuse that feature (*i.e.*, what benefit the criminals get).
- what *enables* the criminal to derive the benefit (i.e the strengths of the feature as well as its vulnerabilities). For example, a safe, flexible, efficient service that is well regulated is as attractive to the criminal as it is to the law abiding citizen).
- The typology could also identify the *harms* caused.

The WGTYP can then make further judgements about whether successful ML/TF activities within one feature are less harmful than successful ML/TF activities via another.

The GTA could also be used as a determining factor of how the WGTYP determines topics for future typologies projects and workshops. The WGTYP could to do fewer projects, but those which have a larger impact on the need for global attention or action. The WGTYP should seek to identify those threats which are not only misunderstood, but those which pose the largest harm.

Future FATF Strategic Surveillance Surveys: Questions may be asked in different ways in order to collect relevant information on *features, drivers/enablers, harms and measures*. Jurisdictions may choose to collect that data by adjusting their internal collection processes, such as analysing case studies in terms of the features/sub-features, identified reasons for misuse, resulting harms and successful measures. The WGTYP will have to consider how the current surveillance mechanism can be used a data collection tool for continued analysis of the ML/TF threats.

ANNEX C: CRIME AND TERRORISM – HARM FRAMEWORK

The harms of crime and terrorism are significant and can be seen as occurring at three levels – individual and local, community and regional and national and international.

At the individual and local level, the use of commodities or services controlled by criminals has a negative impact on individuals in terms of health, personal wealth and quality of life. Damage caused to individuals includes the effect of these undesirable behaviours on others, *i.e.*, young people drawn into crime by easy money, power or sense of affiliation. There is also a direct negative impact on those that are personally living criminal lifestyles, as they face a higher risk of physical violence. Terrorism has also developed to seriously threaten the safety of individuals. In recent decades, both criminals and terrorists have committed and sponsored kidnapping, and used violence and intimidation to coerce innocent individuals into facilitating crime and to achieve political or military goals.

At the community and regional level, there is damage to the reputations of areas in which illegal activity is prevalent and financial losses to legitimate businesses due to being the victims of crime and terrorism. In addition, terrorist attacks also devastate the local areas that are targeted. The long-term effect of these activities serves to undermine public confidence in law enforcement and the wider criminal justice system.

Finally, at the national and international level, the global reach of organised crime and terrorism has weakened economies,[33] corrupted governments and caused or exacerbated the failure of states. Jurisdictions that contain or suffer from organised crime and terrorism may also suffer from the reputational and financial impact on their institutions and economies. The prevalence of extremist views associated with terrorism can also damage social fabric.

The chart within this Annex sets these harms out as they apply to crime and terrorism, and makes cross references from them to the type of harm.

These harms relate predominantly to predicate criminal activity or terrorism, rather than the subsequent ML/TF. However, as ML/TF is a facilitator of these activities, in many cases it will be difficult to extract the harms completely.

33 For example, the terrorist attacks resulting in devastating effects on tourist industries in some countries.

	INDIVIDUAL/LOCAL	COMMUNITY/REGION	NATIONAL/INTERNATIONAL
PHYSICAL	**Individual death, injury or illness:** • Through use of commodities or services controlled by organised criminals (*e.g.,* through drug abuse, or as a facilitated illegal migrant). • Through being the victim of terrorist activity (for example an attack or a kidnapping). • As a consequence of personal involvement in organised criminal activity (*e.g.,* as a victim of intergang violence) or as a terrorist (*e.g.,* as a suicide bomber).	**Incidence of deaths, injuries or illnesses within a particular community or geographical area:** • Through use of commodities or services controlled by organised criminals (*e.g.,* concentrations of drug related deaths, or of sexually exploited human trafficking victims). • As a consequence of direct involvement in organised criminal activity (*e.g.,* drug debt or terrorism related kidnaps or spates of organised crime or terrorism-linked violence).	**Levels and patterns of deaths, injuries, illnesses within a country:** • Through use of commodities or services controlled by organised criminals (*e.g.,* total annual drug related deaths). • As a consequence of direct involvement in organised crime (*e.g.,* drug debt or terrorism kidnaps or spates of organised crime/terrorism-linked violence).
SOCIAL	**Damage to individuals through their criminal and other undesirable behaviours, and the effects on others:** • Behaviour of those involved in organised crime or using its commodities or services (*e.g.,* propensity to violence, prolific offending resulting from drug addition, spiralling criminal behaviour). • Negative influences on others (*e.g.,* young people drawn to crime or terrorism by easy money, power or sense of affiliation). • Effects on victims of organised criminal or terrorism (*e.g.,* distress/inconvenience caused to a victim of terrorism or identity fraud)	**Damage to sense of 'well-being' in a particular geographical area, or within or between ethnic or other identifiable social groups:** • As a result of organised criminal or terrorist activity (*e.g.,* low levels of confidence in local law enforcement and wider criminal justice system). • As a result of the availability of its commodities or services (*e.g.,* high rates of acquisitive crime near drug markets leading to increased fear of crime and community tension). • As a result of the prevalence of extremist views.	**Damage to national society, undermining social responsibility, belief in the rights of others, respect for the law:** • As a consequence of serious criminal or terrorist activity, or the availability of its commodities or services (*e.g.,* 'low-level' criminal/non-compliant behaviours, such as 'recreational' drug use or personal tax evasion; unwillingness to support the criminal justice system, for example to act as witness to a crime or to perform jury service)/ • As a consequence of the prevalence of extremist views.

	INDIVIDUAL/LOCAL	COMMUNITY/REGION	NATIONAL/INTERNATIONAL
ENVIRONMENTAL	**Degeneration of a locality (inc. a single property):** • As a result of organised criminal activities (*e.g.,* physical damage to a dwelling or other premises used to manufacture or sell drugs, or through its use for prostitution linked to human trafficking) • As a result of it being the site of a terrorist attack. • As a result of the actions of those using its commodities or services (*e.g.,* discarded drug paraphernalia).	**Damage to an area (*e.g.,* an estate, neighbourhood, town):** • As a result of organised criminal or terrorist activity, including any hidden health and safety hazards (*e.g.,* unsafe disposal of chemical waste from drug production or presence of explosive materials). • As a result of it being the site of a terrorist attack. • As a result of those using organised crime's commodities or services (*e.g.,* the creation of deprived/'abandoned' areas through the concentration of drug users or illegal immigrants, leading to further degeneration).	**Damage to the nation as a whole, or to large areas, or to other countries:** • As a result of organised criminal activity, or the availability of its commodities or services (*e.g.,* demand in some countries for class A drugs causing deforestation in South America). • As a result of widespread terrorist attacks.
ECONOMIC	**Costs to/economic impacts on individuals or families:** • Using organised crime commodities or services (*e.g.,* loss of current employment and long-term employability through drug addiction). • Costs to victims and the wider public (*e.g.,* from thefts, costs of security, higher insurance premiums and other costs passed on to consumers).	**Costs to/economic impacts of organised criminal and terrorist activities on businesses, services & communities in a particular town, city or region:** • On legitimate businesses due to organised crime (*e.g.,* losses as a result of fraud or robbery, or loss of trade or failed businesses as a result of illegitimate). • On legitimate businesses due to terrorism (*e.g.,* losses as a result of not being able to trade because of damaged premises or deterred customers, and the cost of rebuilding damaged property). • To local public & social services (*e.g.,* costs of health services for criminals and victims of crime and terrorism, and costs of repairing damaged property and infrastructure). • To local communities (*e.g.,* through overall downturn in trade or lost opportunities for inward investment).	**Costs to/economic impacts on the nation of organised criminal and terrorist activities:** • Direct (*e.g.,* consequences of illegal working on the availability of jobs and competitiveness of national industry; loss of direct and indirect tax and duty revenue from smuggling of goods and from fraud). • Indirect (*e.g.,* public expenditure required to combat organised crime and terrorism through law enforcement and through regulation and controls, and the costs of repairing damaged property and infrastructure).

	INDIVIDUAL/LOCAL	COMMUNITY/REGION	NATIONAL/INTERNATIONAL
STRUCTURAL	**Damage to individual perceptions of the integrity of public and private institutions and systems:** • As a result of organised criminal activity (*e.g.,* fear of using new technology due to perceived risk of online fraud). • As a result of terrorist activity (*e.g.,* fear of particular locations due to perceived risk of terrorist attack or disinclination towards them due to previous attack). • As a result of the actions of those using organised crime's commodities and services (*e.g.,* individuals losing faith in ability of bodies to protect them/their property from the consequences of criminality, including organised crime).	**Damage to commonly shared perceptions of the integrity of public and private institutions and systems:** • As a result of organised criminal activity, or the actions of those using its commodities and services (*e.g.,* local areas dominated by seemingly 'untouchable' criminal elements, or local political or business leaders corrupted by or under the malign influence of organised crime). • As a result of terrorist activity (*e.g.,* local areas infiltrated by extremist views).	**Damage to perceptions of the country internationally:** • As a result of organised criminal activity (*e.g.,* concerted attack on the financial sector including subprime mortgage fraud and 'boiler room' fraud). • As a result of the actions of those using commodities and services or organised crime (*e.g.,* widespread organised illegal immigration undermining the integrity of the borders). • As a result of the prevalence of terrorism.

ANNEX D: SUMMARY OF MEASURES FOR CONSIDERATION[34]

Feature/Sub-feature	*Measures for consideration*
CHAPTER 2: THE ABUSE OF CASH AND BEARER NEGOTIABLE INSTRUMENTS	
Cash Movements and Smuggling	• Measures contained within SR IX are particularly relevant (including Interpretative Note to include confiscation and international co-operation measures). • Providing for obligatory declaration of travellers' cheques when travelling abroad. • Introducing reporting requirements on other forms of value (*e.g.,* gold coins, casino tokens and access devices). • Implementation of the FATF paper, *International Best Practices on Detecting and Preventing the Illicit Cross-Border Transportation of Cash and Bearer Negotiable Instruments*, issued in 2010. • Strengthening of financial inclusion in low capacity countries with cash intensive economies.
Placement, Including Third Party Accounts	• Measures contained within R.5, R.9, R.10, R.11, R.13, R.19 and SR IV are particularly relevant. (With focus on CDD, record-keeping and the reporting of unusual, suspicious or large-value transactions). • Providing additional powers to law enforcement authorities, such as the use of geographic targeting orders (GTO), where regulators have authority to require a financial institution or a group of financial institutions in a geographic area to file additional reports or maintain additional records beyond the ordinary AML/CFT reporting requirements. • Requirement of CDD on occasional transactions on a risk-sensitive basis, irrespective of the amount involved. • Strengthening of financial inclusion in low capacity countries with cash intensive economies.
Cash Intensive Businesses	• Measures contained within R. 12, R. 16, R. 19, R. 20 and R. 24 are particularly relevant. • Measures contained with the FATF/APG Report, *Vulnerabilities of Casinos and Gaming Sector*, issued in March 2008.Measures contained within the FATF report *ML/TF thought the Real Estate Sector* . • Adoption of the FATF *Risk-Based Approach Guidance for Casinos*, issued in 2008 (*e.g.,* use of surveillance in casinos reduces the risk of chip-based ML schemes). • Tax authorities could play a role in detecting abuse of cash-intensive business through the audit activities.

[34] Please note the focus is on the primary measures for combating abuse of the identified feature, not on measures to implement a complete AML/CFT regime.

Feature/Sub-feature	Measures for consideration
CHAPTER 3: THE ABUSE OF TRANSFER OF VALUE	
The banking system	• Measures contained within R. 3, R. 5, R. 11, R. 38, SR III (including Interpretative Note) and SR VII (including Interpretative Note) are particularly relevant. Beneficiary financial institutions should have mechanism in place for the identification of wire transfers that are not accompanied by complete originator information. • Compliance with FATF statement on cover payments released in October 2009 to address the potential for misuse of cover payments and to promote greater transparency of cross-border wire transfers. • Where appropriate, adopting laws authorising or requiring banks to deny opening an account to certain types of customers especially known criminals. • Implementation of the FATF paper, *International Best Practices on Confiscation (Recommendations 3 and 38)*, issued in February 2010. • Implementation of the FATF paper, *International Best Practices on "Freezing of Terrorist Assets*, issued in October 2003.
Money transfer businesses and alternative remittance system	• Measures contained within R.4-16, R.21-25, SR VI (including interpretative note) and SR VII are particularly relevant. (taking into account the differences in nature between providers of these services and other financial sectors such as banking and must be balanced with objectives such as the provision of basic financial services to persons who do not have access to formal financial institutions.) • Adoption of FATF RBA guidance on money service businesses issued in July 2009. • Implementation of the FATF paper, *International Best Practices on Combating the Abuse of Alternative Remittance Systems*, issued in June 2003 and similar guidance issued by regional bodies. • Effective collaboration between law enforcement and regulatory agencies to identify and prosecute businesses that facilitate ML, including publicity of these actions. • Increasing the transparency of money transfer businesses and alternative remittance systems, including beneficial ownership. • Authorities should make the use of the formal sector more attractive (*e.g.,* take steps that reduce transaction cost).
The international trade system, including trade based money laundering	• Implementation of the FATF paper, *International Best Practice on Trade-Based Money Laundering*, issued in June 2008. • Consideration of measures contained in the FATF report, *Money Laundering Vulnerabilities of Free Trade Zones*, issued in March 2010. • Creation of mechanisms and channels to improve national and international cooperation with competent authorities as well as with the private sector. • Improved training programmes for global trade services departments to strengthen their trade finance policies and activities. • Establishing programs to build expertise and raise awareness with trade, investigative, prosecutorial and

Feature/Sub-feature	Measures for consideration
	regulatory authorities to identify TBML techniques. • Disseminating typologies, red-flag indicators and sanitised case studies to private sector and competent authorities. • Establishing clear and effective gateways to facilitate the international exchange of trade data amongst authorised counterparts. Considering establishing a trade transparency unit. • Requirements for transparency between goods and value for financial service providers (banks see import documentation as well as invoices). • Sharing information with domestic and foreign agencies (with specific emphasis on import and export information), and then acting on this.
Third party business structures, charities and other legal entities	• Measures contained within R. 33, and 34 and SR VIII (including interpretative note) are particularly relevant. • Ensuring transparency with regards to beneficial ownership. • Implementation of the *Risk Based Approach (RBA) Guidance for Trusts and Company Service Providers (TCSP)*, issued in June 2008. • Establishing registries of trusts to assist investigators and the financial sector in establishing beneficial ownership. • Establishing a system of continuous screening of legal persons in order to tackle misuse. • Implementation of the FATF paper, *International Best Practices on Combating the Abuse of Non-Profit Organisations*, issued in October 2002.
Retail payment systems and the ATM network (including new payment methods)	• Measures contained within R. 5, R.8, R. 9, R. 10, R. 11, R. 13, R. 19, SR. IV and SR. VI are particularly relevant. • Making electronic payment systems a part of national AML/CFT systems (including on the legislative level). • Limiting the value that can be funded, stored and spent. • Monitoring of accounts and reporting suspicious activity. • Limits on cross-border access of funds. • Maintaining transaction records with payer and recipient. • Interaction among industry/regulatory /enforcement during product development to cut out vulnerabilities at design level as far as possible (“product testing”). • Consideration of measures contained in the FATF report, *ML/TF Vulnerabilities of Commercial Websites and Internet Payment Systems*, issued in June 2008. • Consideration of measures contained in the FATF report, *New Payment Technologies*, issued in October 2006.

Feature/Sub-feature	Measures for consideration
CHAPTER 4: THE ABUSE OF ASSETS/STORES OF VALUE	
Overall measures	• Implementation of the FATF paper, *International Best Practices on Confiscation (Recommendations 3 and 38)*, issued in February 2010. • Introduction of non-conviction based asset confiscation (civil confiscation). • Taxing criminal assets where civil confiscation is not feasible. • Introducing asset forfeiture custodian regimes or asset management offices to prevent the dissipation of confiscated assets. • Reinvestment of confiscated assets in law enforcement work to encourage further confiscation activity. • Establishing specialised units or dedicated personnel with training in specialised financial investigation techniques. • Placing legal restrictions for criminals from holding certain types of assets.
Financial products (including insurance, investment & saving products etc)	• See chapter 4 overall measures. • Adoption of FATF guidance on the risk-based approach for the life insurance sector published in October 2009. • Information sharing with the financial sector, including on red flag indicators and typologies. • Consideration of measures contained within the FATF report, *ML/TF in the Securities Sector*, issued October 2009.
Moveable goods	• See chapter 4overall measures • Measures contained within R. 12, 16, 20 and 24 are particularly relevant.
Real estate (ownership and leasing of land and building)	• See chapter 4, "Overall Countermeasures". • Measures contained within R. 12 and 16. • Adoption of the FATF *Risk-Based Approach Guidance for Real Estate,* issued in June 2008. • Measures contained within the FATF report, *ML/TF thought the Real Estate Sector*. • Considering whether to bring leasing agents within the scope of regulation in order to disrupt criminal activity. • Bringing national property -measures into the scope of national AML/CFT regimes (*e.g.,* land registry).
CHAPTER 5: THE ABUSE OF GATEKEEPERS	
Professionals and insiders	• Measures contained within R. 12 and 16 are particularly relevant. • Adoption of the FATF *Risk-Based Approach Guidance for Legal Professionals,* issued in October 2008. • Adoption of the FATF *Risk-Based Approach Guidance for Accountants*, issued in June 2008. • Appropriate publicity, sharing information and raising awareness on ML/TF threats. • Creation of a dedicated function with responsibility to receive and analyse STRs from each profession may help to build specialisation/expertise leading to enhanced result.

Feature/Sub-feature	Measures for consideration
	• Strong codes of conduct and codes of ethics for these professionals (supported by their supervisory and regulatory bodies) which include AML/CFT components and corresponding disciplinary action. • Appropriate sanctions and publicity for the sanctions by competent authorities. • Take appropriate steps to lessen the negative impact of privilege of confidentiality in lawyer/client relationship on AML/CFT effectiveness. • Insiders – measures contained within R.14, 15 and 23 are particularly relevant.
PEPs	• Measures contained within R. 1, 3, 6, 13, 15, 16, 23, 24, 26, 30, 36-40 are particularly relevant. • Ratifying and implementing relevant international conventions against corruption (*e.g.,* the *UN Convention against Corruption* [UNCAC], the *OECD Convention against Bribery of Foreign Officials*, the *Inter-American Convention against Corruption*, etc.). • Widening the definition of PEPs to include domestic PEPs and enhanced due diligence on them (see Interpretive Note to R. 6). • Considering the removal of immunities from criminal prosecution for heads of state, government and political figures, where feasible. • Creation of an independent, dedicated anti-corruption body and asset registries for public sector officials and introduction of financial disclosure requirements for PEPs.
CHAPTER 6: THE ABUSE OF ENVIRONMENTAL / JURISDICTIONAL ASPECTS	
Overall countermeasures	• Measures contained within all FATF Recommendations are relevant. • Measures contained within R. 21 to include appropriate countermeasures to include: - Stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories, to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from these countries; - Enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious; - In considering requests for approving the establishment in countries applying the countermeasure of subsidiaries or branches or representative offices of financial institutions, taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems; - Warning non-financial sector businesses that transactions with natural or legal persons within that country might run the risk of ML. - Limiting business relationships or financial transactions with the identified country or persons in that country. • Highly vulnerable jurisdictions must take internal measures to deal with the vulnerabilities. • Extending international assistance to hep the country to establish an effective AML/CFT regime.

Feature/Sub-feature	Measures for consideration
Variable standards and controls	• Measures contained within all FATF Recommendations are relevant. - Stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories, to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from these countries; - Enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious; - In considering requests for approving the establishment in countries applying the countermeasure of subsidiaries or branches or representative offices of financial institutions, taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems; - Warning non-financial sector businesses that transactions with natural or legal persons within that country might run the risk of ML. • Limiting business relationships or financial transactions with the identified country or persons in that country. • Strengthening financial inclusion in low capacity countries. • Delivery of technical and financial assistance and capacity building. • Denying access to their financial sector or denying banking licenses to foreign banks that do not have adequate AML/CFT systems.
Cash intensive economies	• See measures under Chapter 2. • Strengthening financial inclusion in low capacity countries. • Establishing appropriate and rational thresholds with respect to AML/CFT reporting requirements for large-value cash transactions and cross-border movements of cash. • Customer identification on cash deposits and/or withdrawals, challenging to implement but potentially beneficial.
Major financial centres, tax havens & offshore banking centres	• Measures contained in all FATF Recommendations are relevant. • Ensuring that financial secrecy laws do not inhibit the implementation of the FATF standards (*i.e.,* R. 4). • Ensuring that law enforcement have the ability to obtain information and compel documents (*i.e.,* R. 28) • Ensuring that financial regulators have the ability to obtain information and compel documents (*i.e.,* R. 29). • Identification of the beneficial owner (*i.e.,* R. 5) • For tax havens and offshore banking centres, Recommendation 18 disallowing shell banks and banking relationships with such entities is noteworthy. • Strong international cooperation – Measures contained within Recommendations 36-40.
High-risk and conflict zones (e.g., areas known to have a concentration of terrorist or	• Measures contained within SR VI, SR VIII and SR IX are particularly relevant. • Implementation of the FATF paper, *International Best Practices on Combating the Abuse of Alternative*

Feature/Sub-feature	Measures for consideration
criminal activity)	*Remittance Systems*, issued in June 2003, and similar guidance issued by regional bodies. • Implementation of the FATF paper, *International Best Practices on Combating the Abuse of Non-Profit Organisations*, issued in October 2002. • Implementation of the FATF paper, *International Best Practices on Detecting and Preventing the Illicit Cross-Border Transportation of Cash and Bearer Negotiable Instruments*, issued in 2010. • Effective regulation and supervision of money transfer businesses and alternative remittance services based on monitored and identified risks. • Providing guidance to the donor communities and charitable sector on risk factors, risk mitigation practices and role of government.
Jurisdictions with high levels of corruption	• Measures listed to address PEPs as gatekeepers are relevant here. See Chapter 5 • Jurisdictions should respect the principles of transparency and good governance, participate actively in regional or international anti-corruption initiatives, and commit themselves to implementing international legal frameworks such as the *United Nations Convention against Corruption*.

Table note:

R. = Recommendation

SR = Special Recommendation

FATF/OECD
July 2010

www.fatf-gafi.org