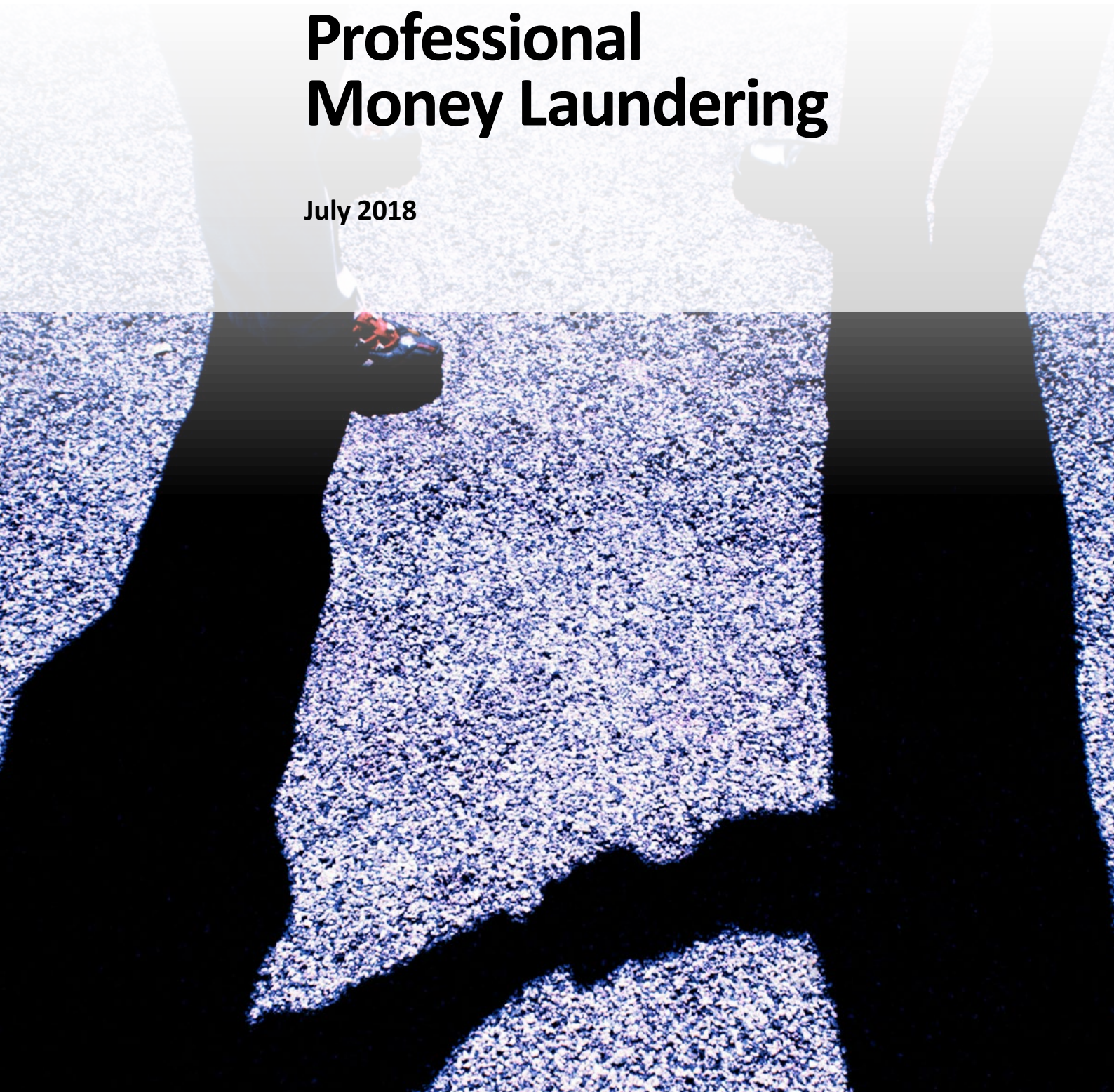FATF REPORT

Professional
Money Laundering

July 2018

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, terrorist financing and the financing of proliferation of weapons of mass destruction. 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 **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

TABLE OF CONTENTS

Boxes

TABLE OF ACRONYMS

CFATF	Caribbean Financial Action Task Force
EAG	Eurasian Group
FIU	Financial Intelligence Unit
LEA	Law Enforcement Agency
MENAFATF	Middle East and North Africa Financial Action Task Force
ML	Money Laundering
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MVTS	Money Value Transfer Service
PML	Professional Money Launderer
PMLO	Professional Money Laundering Organisation
PMLN	Professional Money Laundering Network
OCG	Organised Crime Group
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider

EXECUTIVE SUMMARY

This is the first time the FATF is undertaking a project which concentrates on professional money launderers (PMLs) that specialise in enabling criminals to evade anti-money laundering and counter terrorist financing safeguards and sanctions in order to enjoy the profits from illegal activities. The report aims to describe the functions and characteristics that define a "professional" money launderer, namely those individuals, organisations and networks that are involved in third-party laundering for a fee or commission. This report is therefore focused on money laundering *threats* as opposed to *vulnerabilities*, and it addresses criminal actors, including organised crime groups that specialise in the provision of professional money laundering services and complicit actors who are knowingly involved, or are deliberately negligent, in the laundering process. While PMLs may act in a professional capacity (e.g. lawyer, accountant) and serve some legitimate clients, the report aims to identify those actors who serve criminal clients whether on a full-time or part-time basis.

PMLs provide services to criminals and organised crime groups by laundering the proceeds of their illegal activities. As the main purpose of PMLs is to facilitate money laundering, they are rarely involved in the proceeds-generating illegal activities. Instead, they provide expertise to disguise the nature, source, location, ownership, control, origin and/or destination of funds to avoid detection. PMLs generally do not differentiate between drug dealers, fraudsters, human traffickers or any other criminal with a need to move or conceal ill-gotten gains. These are all potential PML clients. PMLs operate under a number of business models and may be individuals; criminal organisations with a clear structure and hierarchy; or networks of loosely affiliated members. Providing services to criminals and organised crime groups, PMLs are criminal actors, profiting from these money laundering activities.

PMLs may provide the entire infrastructure for complex money laundering schemes (e.g. a 'full service') or construct a unique scheme tailored to the specific needs of a client that wishes to launder the proceeds of crime. These PMLs provide a menu of generally applicable services, with the result that the same laundering techniques (and potentially the same financial channels and routes) may be used for the benefit of multiple organised crime groups. As such, professional money laundering networks may act transnationally in order to exploit vulnerabilities in countries and particular businesses, financial institutions, or designated non-financial businesses or professions. PMLs, themselves, pose a threat to the financial system, as they facilitate money laundering and criminality more broadly, profiting from these illegal activities. The results of FATF's fourth round of mutual evaluations reveal that many countries are not sufficiently investigating and prosecuting a range of money laundering activity, including third-party or complex money laundering. Many countries continue to limit their investigations to *self-launderers*: criminals who

launder the proceeds of drug trafficking, fraud, tax evasion, human trafficking or other criminality. While this may address in-house or self-laundering, it does not impact on those specialised in providing criminals with money laundering services. PMLs, professional money laundering organisations and professional money laundering networks can survive law enforcement interdiction against any of its criminal or organised crime group clients, while still standing ready to support the next criminal clientele. Effective dismantling of PMLs requires focused intelligence collection and investigation of the laundering activities, rather than the associated predicate offences of the groups using the services of the PMLs. The dismantling of PMLs, can impact the operations of their criminal clients, and can be an effective intervention strategy against numerous criminal targets.

This report identifies the specialist skill sets that PMLs offer their clients in order to hide or move their proceeds, and provides a detailed explanation of the roles performed by PMLs to enable authorities to identify and understand how they operate. This can include locating investments or purchasing assets; establishing companies or legal arrangements; acting as nominees; recruiting and managing networks of cash couriers or money mules; providing account management services; and creating and registering financial accounts. This report also provides recent examples of financial enterprises that have been acquired by criminal enterprises or co-opted to facilitate ML. The analysis shows that PMLs use the whole spectrum of money laundering tools and techniques; however, the report specifically focuses on some of the common mechanisms used to launder funds, such as trade-based money laundering, account settlement mechanism and underground banking.

The project team also examined potential links between PMLs and terrorist financing, however, there was insufficient material provided to warrant a separate section on this topic. The *Khanani* provides the clearest example of a professional money laundering organisation, providing services to a UN designated terrorist organisation. One delegation also noted potential links between a loosely affiliated professional money laundering network and a domestically designated terrorist organisation. However, the vast majority of cases submitted relate to money laundering, rather than terrorist financing.

The non-public version report also explores unique investigative tools and techniques that have proved successful in detecting and disrupting PMLs to guide countries that are seeking to address this issue. The report includes a number of practical recommendations that are designed to enhance the identification and investigation of PML; identify strategies to disrupt and dismantle these entities; and identify steps to prevent PML. Combatting these adaptable PMLs requires concerted law enforcement and supervisory action at the national level, appropriate regulation and effective international co-operation and information exchange. This report emphasises the need for a more co-ordinated operational focus on this issue at a national level, and the importance of effective information sharing between authorities at an international level. The report also identifies the information and intelligence required to successfully identify, map, and investigate PMLs, with the objective of disrupting and dismantling those involved in PML and their criminal clientele.

This report intends to assist authorities at jurisdictional level target PMLs, as well as the structures that they utilise to launder funds, to disrupt and dismantle the groups that are involved in proceeds-generating illicit activity so that crime does not pay.

PROFESSIONAL MONEY LAUNDERING

SECTION I: INTRODUCTION

Purpose, Scope and Objectives

The FATF has conducted a number of studies on money laundering (ML) risks. The resulting reports have usually examined ML threats associated with particular proceeds generating offences or vulnerabilities associated with entities covered under the FATF Standards. This report assesses the threats associated with professional money launderers (PMLs), and does not assess ML vulnerabilities that are covered in other FATF reports. Specifically, the report aims to:

- raise awareness of the unique characteristics of professional money laundering (PML);

- understand the role and functions of those involved in PML;

- understand the business models and specific functions performed by PMLs;

- understand how organised crime groups (OCGs) and terrorists use the services of PMLs to move funds;

- identify relevant ML typologies and schemes;

- develop risk indicators for competent authorities and the private sector that are unique for PMLs; and

- develop practical recommendations for the detection, investigation, prosecution and prevention of PML.

Structure of the Report

Sections II and **III** provide the framework for the report, including key characteristics of PML; differences between individuals, organisations and networks involved in PML; and an explanation of the roles performed by those involved. The aim of these sections is to ensure a consistent dialogue on this topic as countries deepen their understanding of this issue.

Sections IV, **V** and **VI** highlight the main types of dedicated ML networks, including the types of complicit and criminal financial services providers and other professional intermediaries generally involved in PML, and common mechanisms used to launder funds. The types of information within these sections should not be considered finite, as PMLs utilise all ML tools and techniques available to them and continue to adapt their methods to take advantage of regulatory and enforcement gaps.

Methodology

This project was co-led by the Russian Federation and the United States and incorporates input from a variety of delegations across the FATF's Global Network. The project team received submissions from Argentina, Australia, Belgium, Canada, China, Germany, Israel, Italy, Malaysia, the Netherlands, the Russian Federation, Singapore, Spain, the United Kingdom, the United States, EAG Members (Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan), MONEYVAL (Ukraine), MENAFATF (Lebanon), CFATF (Belize) and EUROPOL.

Authorities provided detailed information, including from risk assessments and case examples of various schemes arranged by PMLs, strategic analysis outcomes, information on internal organisational and behavioural aspects of PMLNs and investigative techniques. The report includes select country examples to provide the necessary context.

Input was also gathered at the Middle East and Africa Joint Typologies and Capacity Building Workshop in Rabat, Morocco, from 22-25 January 2018, and input and feedback gathered at the FATF Joint Experts Meeting held in Busan, Republic of Korea, from 1-4 May 2018. The findings of this report also rely on feedback from financial intelligence units (FIUs) and law enforcement agencies (LEAs), based on their experiences in investigating PMLs.

There has been sparse research on this subject. However, the project team did take into consideration previous and ongoing work by the FATF on operational issues, including the 2012 *FATF Guidance on Financial Investigations*, 2013 *FATF Report on ML and TF Vulnerabilities of Legal Professionals* and the 2018 *Joint FATF/Egmont Report on the Vulnerabilities Linked to the Concealment of Beneficial Ownership*.

SECTION II: CHARACTERISTICS OF PROFESSIONAL MONEY LAUNDERING

This section of the report outlines the key characteristics, which make PML unique, and helps to frame the scope of this report. **Section III** then provides a list of specialised services, which include specific roles or functions performed by various individuals. The report has attempted to avoid the use of formal titles (e.g. controller, enabler and facilitator), as multiple and inconsistent terminology is used globally, which leads to confusion when describing these functions. **Section III** provides a business model demonstrating how PMLs generally conduct financial schemes.

Key Characteristics

PML is a subset of third-party ML. The FATF defines third-party ML as the laundering of proceeds by a person who was not involved in the commission of the predicate offence[1]. The main characteristic that makes PML unique is the provision of ML services in exchange for a commission, fee or other type of profit. While the specialisation in providing ML services is a key feature of PMLs, this does not mean that PMLs are not also involved in other activities (including legal businesses).

---

[1] FATF Methodology 2013, footnote to Immediate Outcome 7.

Similarly, this does not mean that they exclusively only launder illicit proceeds. PMLs also use specialised knowledge and expertise to exploit legal loopholes; find opportunities for criminals; and help criminals retain and legitimise the proceeds of crime.

Given that PMLs are third-party launderers, they are often not familiar with the predicate offence (e.g. narcotics or human trafficking) and are generally not concerned with the origins of the money that is moved. Nonetheless, PMLs are aware that the money that they move is not legitimate. The PML is concerned primarily with the destination of the money and the process by which it is moved. They are used by clients in order to create distance between those perpetrating the crimes and the illicit proceeds that they generate as profit, or because the criminal clients do not have the knowledge required to reliably launder the money without law enforcement detection.

Ultimately, PMLs are criminals, who often operate on a large scale and conduct schemes that are transnational in nature. The term "PMLs" is not intended to include unwitting or passive intermediaries who are exploited to facilitate an ML scheme. Other features of PMLs are that they sometimes operate on a large scale and often conduct schemes that are transnational in nature.

Commissions / Fees

A number of different and overlapping factors affect the fee paid to PMLs or the commission they receive for their services. The fee will often depend on the complexity of the scheme, methods used and knowledge of the predicate offence. The rate may change based on the level of risk that PMLs assume. For example, commission rates are often influenced by the countries or regions involved in the scheme, as well as other factors such as:

- the reputation of the individual PML;
- the total amount of funds laundered;
- the denomination (i.e. value) of the banknotes (in cases involving cash);
- the amount of time requested by a client to move or conceal funds (for example, if the laundering needs to be done in a shorter time period, the commission will be higher); and
- the imposition of new regulation(s) or law enforcement activities.

To obtain commission for their services, PMLs may (i) take commission in cash in advance, (ii) transfer a portion of money laundered to their own accounts or (iii) have the commission integrated into the business transaction.

Advertising / Marketing

Advertising and marketing of services can occur in numerous ways. Often, this involves the PMLs actively marketing their services by 'word-of-mouth' (through an informal criminal network). Criminal links and trust developed through previous criminal engagement also strengthens bonds and can encourage further co-operation. Authorities have also identified the use of posted advertisements for PML services on the Dark Web.

Record Keeping (Shadow Accountancy)

Law enforcement has reported that PMLs often keep a shadow accounting system that contains detailed records with code names. These unique accounting systems may use detailed spreadsheets that track clients (using code names); funds laundered; the origin and destination of funds moved; relevant dates; and commissions received. PMLs may either store their records electronically (e.g. a password-protected Excel spreadsheet) or use paper records. These records represent an invaluable resource for investigators.

Individuals, Organisations and Networks

PMLs can belong to one of three categories:

1.   An **individual PML,** who possesses specialised skills or expertise in placing, moving and laundering funds. They specialise in the provision of ML services, which can also be performed while acting in a legitimate, professional occupation. These services can include, but are not limited to, the following: accounting services, financial or legal advice, and the formation of companies and legal arrangements (see *specialised services*, below). Individual PMLs often spread their risks across diverse products, and carry out business activities with several financial specialists and brokers (see examples below).

2.   A **Professional money laundering organisation (PMLO)**, which consists of two or more individuals acting as an autonomous, structured group that specialises in providing services or advice to launder money for criminals or other OCGs. Laundering funds may be the core activity of the organisation, but not necessarily the only activity. Most PMLOs have a strict

hierarchical structure, with each member acting as a specialised professional that is responsible for particular elements of the ML cycle (see **Section III**).

3.　　A **Professional money laundering network (PMLN)**, which is a collection of associates or contacts working together to facilitate PML schemes and/or subcontract their services for specific tasks. These networks usually operate globally, and can include two or more PMLOs that work together. They may also operate as informal networks of individuals that provide the criminal client with a range of ML services. These interpersonal relationships are not always organised, and are often flexible in nature.

These extensive PML networks are able to satisfy the demands of the client by opening foreign bank accounts, establishing or buying foreign companies and using the existing infrastructure that is controlled by other PMLs. Collaboration between different PMLs also diversifies the channels through which illicit proceeds may pass, thereby reducing the risk of detection and seizure.

PMLOs work with OCGs of all nationalities, on a global basis or in a specific region, often acting as a global enterprise. The same PML can be used to facilitate ML operations on behalf of several OCGs or criminal affiliates. They are highly skilled and operate in diverse settings, adept at avoiding the attention of law enforcement. One relevant case has been identified demonstrating that the same money launderers provided services to both OCGs and terrorist organisations (see Box 1, below).

Box 1. Khanani Money Laundering Organisation

The Altaf Khanani Money Laundering Organisation (MLO) laundered illicit proceeds for other OCGs, drug trafficking organisations and designated terrorist groups throughout the world. The Khanani MLO was an OCG composed of individuals and entities operating under the supervision of Pakistani national, Altaf Khanani, whom the US Drug Enforcement Administration (DEA) arrested in 2015. The Khanani MLO facilitated illicit money movements between Pakistan, the United Arab Emirates (UAE), the United States, the United Kingdom, Canada, Australia and other countries. It was responsible for laundering billions of dollars in criminal proceeds annually.

The Khanani MLO offered ML services to a diverse clientele, including Chinese, Colombian and Mexican OCGs, as well as individuals associated with a US

---

domestically designated terrorist organisation. The Khanani MLO has also laundered funds for other designated terrorist organisations. Specifically, Altaf Khanani, the head of the Khanani MLO and Al Zarooni Exchange, has been involved in the movement of funds for the Taliban, and Altaf Khanani is known to have had relationships with Lashkar-e-Tayyiba, Dawood Ibrahim, al-Qa'ida and Jaish-e-Mohammed. Furthermore, Khanani was responsible for depositing drug proceeds via bank wires from a foreign business account in an effort to conceal and disguise the nature, source, ownership and control of the funds. Khanani conducted transactions, which involved multiple wire transfers from a number of general trading companies. Khanani's commission to launder funds was 3% of the total value of funds laundered.

The Khanani MLO itself was designated by OFAC in 2015 as a "transnational criminal organisation[1]," pursuant to Executive Order 13581. On the same day, OFAC designated the exchange house utilised by the Khanani MLO, Al Zarooni Exchange. In 2016, the US Treasury's Office of Foreign Assets Control (OFAC) designated four individuals and nine entities associated with the Khanani MLO. On October 26, 2016 Altaf Khanani pleaded guilty to federal ML charges. Approximately USD 46 000 in criminal proceeds was also confiscated from Khanani. In 2017, Altaf Khanani was sentenced to 68 months in prison for conspiracy to commit ML.

Extensive law enforcement co-ordination took place between multiple law enforcement agencies from Australia, Canada and the US who all held a different piece of the puzzle. The designation of Al Zarooni Exchange complements an action taken by the Central Bank of the UAE, with assistance from the AML Unit at Dubai Police General Headquarters, which closely coordinated with the DEA prior to the action taken.

Note: 1. Transnational Criminal Organisation (TCO) is a specific technical term used in the US designation process and is synonymous with organised crime group (OCG), the latter of which is used throughout this report.

Source: United States, Australia, Canada, UAE

OCGs use both outsiders and OCG members to perform ML services on behalf of the group. In cases where there is an in-house component of an OCG that is responsible for ML, these members may receive a portion of the proceeds of the group, rather than a fee or commission. The extent to which PMLs get involved in ML schemes depends on the needs of the criminal group, the complexity of the laundering operation that they wish to execute, as well as the risks and costs associated with such involvement.

When OCGs employ the services of PMLs, they often choose PMLs who are acquainted with persons close to, or within, the OCG network. They can be family members or close contacts. They may also be professionals that previously acted in a legitimate capacity, and who now act as:

- accountants, lawyers, notaries and/or other service providers;
- Trust and Company Service Providers (TCSPs);
- bankers;
- MVTS providers;

- brokers;
- fiscal specialists or tax advisors;
- dealers in precious metals or stones;
- bank owners or insiders;
- payment processor owners or insiders; and
- electronic and cryptocurrency exchanger owners or insiders.

OCGs also make use of external experts on a permanent or ad hoc basis. These experts knowingly operate as entrepreneurs and often have no criminal record, which can aid in avoiding detection. These complicit professionals are increasingly present on the criminal landscape, coming together as service providers to support specific criminal schemes or OCGs (see **Section VI**). PMLs can also provide services to several OCGs or criminal affiliates simultaneously, and are both highly skilled at operating in diverse settings and adept at avoiding the attention of law enforcement.

Compartmentalised relationships also exist, particularly within PMLNs, whereby there may be no direct contact between OCGs and the lead actors responsible for laundering the funds In these instances, transactions are facilitated via several layers of individuals who collect the money (see **Section III**) before funds are handed over to PMLs for laundering.

SECTION III: SPECIALISED SERVICES AND BUSINESS MODELS

PMLs can be involved in one, or all, stages of the ML cycle (i.e. placement, layering and integration), and can provide specialised services to either manage, collect or move funds. PMLOs act in a more sophisticated manner and may provide the entire infrastructure for complex ML schemes or construct a unique scheme, tailored to the specific needs of a client.

There are a number of specialised services that PMLs may provide. These include, but are not limited to:

- consulting and advising;
- registering and maintaining companies or other legal entities;
- serving as nominees for companies and accounts;
- providing false documentation;
- comingling legal and illegal proceeds;
- placing and moving illicit cash;
- purchasing assets;
- obtaining financing;
- identifying investment opportunities;
- indirectly purchasing and holding assets;
- orchestrating lawsuits; and
- recruiting and managing money mules.

Roles and Functions

This section identifies numerous roles and functions that are necessary to the operation of PMLs. These specific functions, outlined below, should not be considered an exhaustive list. Depending on the type of PML, an individual may perform a unique function or perform several roles simultaneously. Understanding these roles is important in order to identify all of the relevant players and ensure that all relevant aspects of PMLs are detected, disrupted and ultimately dismantled.

▪ *Leading and controlling*: There may be individuals who provide the overall leadership and direction of the group, and who are in charge of strategic planning and decision making. Control over ML activities of the group is normally exercised by a leader, but may also be exercised by other individuals who are responsible for dealing with the funds from the time they are collected from clients until delivery (e.g. arranging the collection of cash and organising the delivery of cash at a chosen international destination). These individuals are also responsible for determining the commission charged and paying salaries to other members of the PMLO/PMLN for their services.

▪ *Introducing and promoting*: There are often specific individuals who are responsible for bringing clients to the PMLs and managing communications with the criminal clients. This includes managers who are responsible for establishing and maintaining contact with other PMLOs or individual PMLs that operate locally or abroad. Through the use of these contacts, the PMLO gains access to infrastructure already established by other PMLs.

▪ *Maintaining infrastructure*: These individuals are responsible for the establishment of a range of PML infrastructure or tools. This could include setting up companies, opening bank accounts and acquiring credit cards. These actors may also manage a network of registrars who find and recruit nominees (e.g. front men) to register shell companies on behalf of the client, receive online banking logins and passwords, and buy SIM-cards for mobile communication.

One example of managing infrastructure is the role of a *money mule herder*, who is responsible for recruiting and managing money mules (e.g. via job ads and via a personal introduction), including the payment of salaries to mules. This salary can be paid either as a fee for their money transfer services or as a one-time payment for their services (see **Section IV** for a wider description of money mule networks and the roles within these specific networks).

▪ *Managing documents*: These individuals are responsible for the creation of documentation needed to facilitate the laundering process. In some cases, these individuals are responsible for either producing or acquiring fraudulent documentation, including fake identification, bank statements and annual account statements, invoices for goods or services, consultancy arrangements, promissory notes and loans, false resumes and reference letters.

▪ *Managing transportation*: These individuals are responsible for receiving and forwarding goods either internationally or domestically, providing

customs documentation and liaising with transport or customs agents. This role is particularly relevant to TBML schemes.

- ▪ *Investing or purchasing assets*: Where needed, real estate or other assets, such as precious gems, art or luxury goods and vehicles, are used to store value for later sale. Criminals seek assistance in purchasing real estate overseas, and PMLs have been known to use elaborate schemes involving layers of shell companies to facilitate this.

- ▪ *Collecting*: These individuals are responsible for collecting illicit funds, as well as the initial placement stage of the laundering process. Given that they are at the front end of the process, they are most likely to be identified by law enforcement. However, they often leave little paper trail and are able to successfully layer illicit proceeds by depositing co-mingling funds using cash-intensive businesses. These individuals are aware of their role in laundering criminal proceedings (compared to some money mules, who may be unwitting participants in a PML scheme).

- ▪ *Transmitting*: These specific individuals are responsible for moving funds from one location to another in the PML scheme, irrespective of which mechanism is used to move funds. They receive and process money using either the traditional banking system or MVTS providers, and are also often responsible for performing cash withdrawals and subsequent currency exchange transactions.

General Business Model of Professional Money Laundering Networks

Figure 1. Three stages of professional money laundering

In general, financial schemes executed by PMLs consist of three stages:

Stage 1: Criminal proceeds are transferred to, or collected by, PMLs

In the first stage, funds are transferred, physically or electronically, to PMLs or to entities operating on their behalf. The precise manner of introduction of the funds into the ML scheme varies depending on the types of predicate offence(s) and the form in which criminal proceeds were generated (e.g. cash, bank funds, virtual currency, etc.):

Cash: When illicit proceeds are introduced as currency, they are usually passed over to a cash collector. This collector may ultimately deposit the cash into bank accounts. The collector introduces the cash into the financial system through cash-intensive businesses, MVTS providers or casinos, or physically transports the cash to another region or country.

Bank accounts: Some types of criminal activity generate illicit proceeds held in bank accounts, such as fraud, embezzlement and tax crimes. Unlike drug proceeds, proceeds of these crimes rarely start out as cash but may end up as cash after laundering. Clients usually establish legal entities under whose names bank accounts may be opened for the purposes of laundering funds. These accounts are used to transfer money to a first layer of companies that are controlled by the PMLs.

Virtual Currency: Criminals who obtain proceeds in a form of virtual currency (e.g. owners of online illicit stores, including Dark Web marketplaces) must have e-wallets or an address on a distributed ledger platform, which can be accessed by the PMLs.

Stage 2: Layering stage executed by individuals and/or networks

In the layering stage, the majority of PMLs use account settlement mechanisms to make it more difficult to trace the funds. A combination of different ML techniques may be used as part of one scheme. The layering stage is managed by individuals responsible for the co-ordination of financial transactions.

Cash: ML mechanisms for the layering of illicit proceeds earned in cash commonly include: TBML and fictitious trade, account settlements and underground banking.

Bank Accounts: Funds that were transferred to bank accounts managed by PMLs are, in most cases, moved through complex layering schemes or proxy structures. Proxy structures consist of a complex chain of shell company accounts, established both domestically and abroad. The funds from different clients are mixed within the same accounts, which makes the tracing of funds coming from a particular client more difficult.

Virtual Currency: Criminals engaged in cybercrime or computer-based fraud, as well as in the sale of illicit goods via online stores, often use the services of money mule networks (see Section IV). The illicit proceeds earned from these crimes are often held in the form of virtual currency, and are stored in e-wallets or virtual currency wallets that go through a complex chain of transfers.

Stage 3. Laundered funds are handed back over to clients for investment or asset acquisition

In the last stage, funds are transferred to accounts controlled by the clients of the PML, their close associates or third parties acting on their behalf or on behalf of affiliated legal entities. The PML may invest the illicit proceeds on behalf of these clients in real estate, luxury goods, and businesses abroad (or, in some cases, in countries where the funds originated from). The funds can also be spent on goods deliveries to a country where the funds originated or to a third country.

SECTION IV: TYPES OF DEDICATED ML ORGANISATIONS AND NETWORKS

As mentioned in the previous sections, PMLs may move funds through dedicated networks, utilising multiple mechanisms to move funds. These networks, often used during the placement and layering stages in the laundering cycle, are able to quickly adapt and adjust to shifting environmental factors (such as new regulation) and law enforcement activities. PMLs may also provide detailed guidance to assist with the entire ML scheme and often sell "packages" that contain the instruments and services required to facilitate an ML scheme. This section describes the key types of dedicated ML organisations and networks identified through an analysis of case studies: (i) money transport and cash controller networks; (ii) money mule networks; (iii) digital money and virtual currency networks; and (iv) proxy networks.

Money Transport and Cash Controller Networks

Criminals and OCGs that generate significant amounts of cash often use the services of cash controller networks that are capable of transferring vast sums of cash on their behalf. These international controller networks have the capacity to receive, hand over and transfer criminal proceeds, while charging a processing fee. Generally the structure of these networks consists of individuals who *control, co-ordinate, collect and transmit illicit funds,*[2] and who operate together to negotiate deals with the OCG.

Cash controller networks often orchestrate the laundering of the proceeds of crime for multiple OCGs located worldwide through an account settlement system, whereby illicit proceeds are substituted for legitimate funds. The ML technique employed sometimes involves the transfer of criminal funds through the accounts of unwitting customers who receive funds or payments from abroad. In this scheme, legal funds, which are to be transferred into the bank account of an unwitting third party, are substituted by the launderer with the illicit proceeds of the OCG. The launderer deposits the money in amounts under the reporting threshold to avoid detection.

---

[2] See roles and functions defined in Section III

Figure 2. Money Transport and Cash Controller Network
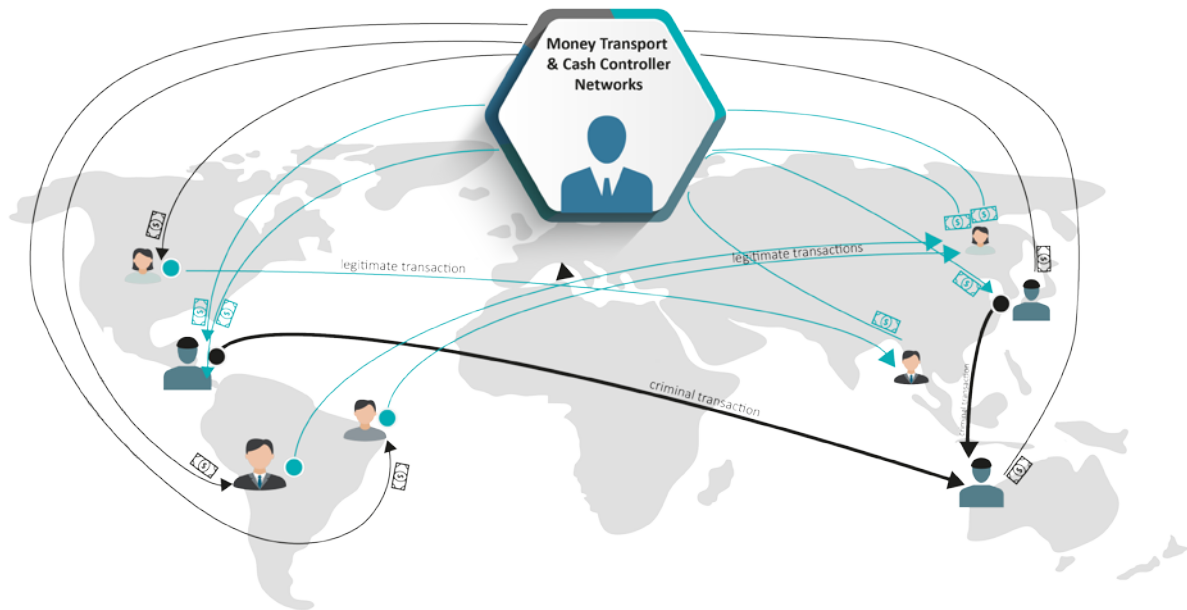
Amounts deposited do not immediately match the overall sums of illicit proceeds. However, in the long term, the value of illicit proceeds collected against the value of deposits tends to be equivalent. Where this is not the case, the PML may resort to other trade-based techniques, such as fake or over invoicing, in order to legitimise the movement of funds between two or more jurisdictions, to balance the system. This technique allows the PML to oversee payments made in another country, without the risk of being detected by holding bank accounts in their own name(s).

If an international cash controller network works with criminals and OCGs operating in different countries, it may easily avoid conducting cross-border transfers of funds, with the support of an account settlement mechanism (see Section V). The chart, below, illustrates the operations of an international cash controller network in four different situations.

Box 2. Cash Controller Network and Account Settlement Scheme

USD 3 000 GREEN: Basic transaction. The Canadian client wants to send money to another client in the UK. It is conducted through the MVTS provider's intermediary.

USD 50 000 RED: An Australian dealer wants to pay its Canadian supplier. The dealer contacts the controller to arrange the transfer. The controller instructs the collector to pick up money. The money is now part of a pool of money in that country under the control of the controller. The controller instructs his Canadian collector to take money from his Canadian pool of money to conduct a money-drop.

USD 45 000 BLUE: The Canadian dealer wants to settle an account in the UK.

The dealer contacts the controller and arranges a pick-up. The collector picks up the money and is instructed to deliver it to a complicit transmitter to place the money into bank accounts (structuring). This increases the Canadian pool of money. The controller then takes money from the UK pool and instructs the UK collector to deliver the money.

USD 18 000 MAROON: A father in India wants to send money to his daughter in Canada. The funds are sent through a hawala network[1]. The collector secures the contract for the controller. The controller then directs his Canadian collector to disperse deposits into the individual`s bank account. He visits three different branches to structure the deposits into the account.
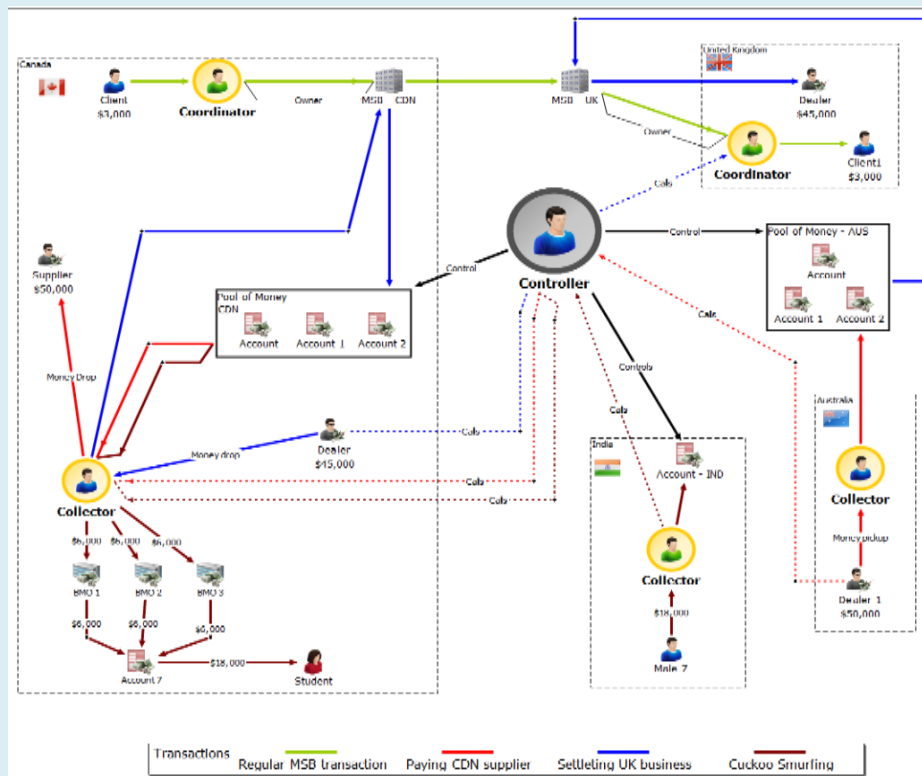
Note: 1. For further information about hawala, see FATF, *Role of Hawala and Other Similar Service Providers in ML and TF*, October 2013

Source: Australia

The laundering of criminal proceeds generated in cash may include the physical transportation of bulk cash. Recent cases show that services to transport cash are also being outsourced to specialised cash transportation networks that are responsible for collecting cash, transporting it to pre-determined locations and facilitating its placement in the financial system. One of the recent examples of efforts taken to combat cash transportation networks that provide services to drug trafficking organisations operating in Europe is EUROPOL's Operation Kandil. The network was responsible for collecting the proceeds of heroin sales throughout Europe (Spain, the Netherlands, Italy and the UK) and transporting this cash to Germany, where it was placed into the financial system through the purchase of second-hand cars, spare parts and equipment.

Box 3. Operation Kandil – Use of Cash Courier Network

In 2016, authorities from Germany, supported by EUROPOL experts, took action against an Iraqi OCG (based in Germany) that was suspected of performing ML services for international heroin traffickers. The operation was preceded by extensive and complex criminal investigations, supported by EUROPOL, which coordinated the law enforcement authorities in France, Spain, Germany and the Netherlands, mirrored by EUROJUST's co-ordination of judicial authorities.

This criminal syndicate, composed mainly of Iraqi nationals, was responsible for collecting the proceeds of heroin sales throughout Europe (Spain, the Netherlands, Italy and the UK) and laundering these funds to the Middle East through Germany, with an estimated total amount of EUR 5 million already laundered.

The criminals' modus operandi involved the use of cash couriers traveling by car to pick up dirty cash all over Europe. This was followed by the use of TBML techniques to transmit the value to the Middle East, primarily through the shipment of second-hand cars; heavy machinery and construction equipment purchased in Germany and exported to Iraq, where the goods were ultimately resold in exchange for clean cash.

The OCG was then able to make use of MVTS services and unregulated financial channels (the hawala system) to integrate and further transfer funds into the regulated financial system. This left virtually no paper trail for law enforcement.

Professional service providers, such as solicitors, accountants and company formation agents, provided the skills and knowledge of financial procedures necessary to operate this scheme. Although, few groups are known to provide these services, they launder large amounts of money, and have a considerable impact on the ability of other OCGs to disguise and invest criminal proceeds. These syndicates are a significant obstacle to tracing criminal assets.

Source: EUROPOL (Germany)

Money Mule Networks

One of the significant elements of many PML schemes is the use of money mules. Money mules are people who are used to transfer value, either by laundering stolen money or physically transporting goods or other merchandise. Money mules may be willing participants and are often recruited by criminals via job advertisements for 'transaction managers' or through online social media interactions. Money mule recruiters are also known as mule 'herders.' Money mules may be knowingly complicit in the laundering of funds or work unwittingly, or negligently, on behalf of a PMLN or OCG. Cyber criminals tailor their recruitment techniques based on the prospective mule's motivations. For example, these criminals will also offer off-the-record cash payments and free travel to incentivise and recruit "witting" mules motivated by easy money and free travel.

Box 4. Use Of Money Mules to Launder Criminal Proceeds

Person A was recruited by a Nigerian syndicate to receive money in her bank accounts. She was promised commissions of up to SGD 5 000 (EUR 3 160) for each transaction. Person A received criminal proceeds from fraud committed in the US and the Bahamas into her bank accounts. Most of the funds were transferred out or withdrawn within a few days of receipt, upon instructions of the Nigerian-based OCG.

Not only did Person A serve as a receptacle for illicit proceeds, she also recruited two other money mules. The control of the mules' bank accounts allowed her to obscure the locations of the illicit proceeds through layering, and enabled her to evade detection as the funds were spread out over multiple accounts. Through this network, Person A and her money mule network received a total of 12 fraudulent wire transfers, amounting to SGD 5 million (EUR 3 16 million) from overseas victims into their bank accounts in Singapore, within a period of six weeks.

Person A was convicted and sentenced to 72 months' imprisonment for receiving stolen property and ML offences.

Source: Singapore

PMLs frequently recruit money mules from diaspora networks and ethnic communities. A sizeable amount of money mule transactions are linked to online illicit stores and cybercrime, such as phishing, malware attacks, credit card fraud, business e-mail compromise and various types of other scams (including romance, lottery and employment scams).

Some money mules are unaware that they are being used to facilitate criminal activity. Unwitting mules are used by OCGs to cash counterfeit checks and money orders or purchase merchandise using stolen credit card numbers or other personal identification information. In some cases, the mules may suspect that the source of the money that they are moving is not legitimate. Such wilfully blind money mules often use income earned to supplement their regular income because they are facing financial difficulties or are motivated by greed.

In the past, money mules have been viewed as low-level offenders, transferring small amounts of cash. However, organised, sophisticated money mule schemes have evolved as a PML mechanism. These money mule networks are controlled by a hierarchical structure, and are well-resourced and highly effective in laundering funds. Money mule networks are usually associated with OCGs that operate cross-border, particularly those involved in cybercrime and the sale of illicit goods through online stores. Typically, these schemes involve criminals that create apparently legitimate businesses, hiring unsuspecting individuals whose jobs involve setting up bank accounts to receive and pass along supposedly legitimate payments. In reality, these unsuspecting individuals act as money mules, processing the criminals' illicit proceeds and wiring them to other criminals.

Money mule networks have been used to open numerous individual bank accounts locally as well as in global financial centres to facilitate the movement of criminal

proceeds. Bank accounts, opened by the mules, serve as the initial layering stage in the laundering process. This indicates that criminals still find the combination of money mule accounts, cash withdrawals and wire transfers to be an effective way to layer proceeds.

Box 5. Avalanche Network

Avalanche is an example of a criminal infrastructure dedicated to facilitating privacy invasions and financial crimes on a global scale. Avalanche was a hosting platform composed of a worldwide network of servers that was controlled via a highly organised central system. This cyber network hosted more than two dozen of the world's most pernicious types of malware and several large scale ML campaigns.

The Avalanche network, in operation since at least 2010, was estimated to serve clients operating as many as 500 000 infected computers worldwide on a daily basis. The monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of USD worldwide.

The Avalanche network offered cybercriminals a secure infrastructure, designed to thwart detection by law enforcement and cyber security experts. Online banking passwords and other sensitive information stolen from victims' malware-infected computers was redirected through the intricate network of Avalanche servers and ultimately to back-end servers controlled by the cybercriminals. Access to the Avalanche network was offered to the cybercriminals through postings on exclusive, dark web criminal forums.

The types of malware and money mule schemes operating over the Avalanche network varied. Ransomware such as Nymain, for example, encrypted victims' computer files until the victim paid a ransom (typically in a form of crypto-currency) to the cybercriminal. Other malware, such as GozNym, was designed to steal sensitive online banking credentials from victims in order to use those credentials to initiate fraudulent wire transfers from the victims' bank accounts.

The ML schemes operating over Avalanche involved highly organised individuals, who controlled server networks and money mules, which were a crucial part of the criminal network. In some cases, the leaders would use a network of individuals to open bank accounts in major global financial hubs to facilitate wire transfers. The mules were often sponsored by the leader of a particular, country-based network and brought to the US, or, they were unwitting individuals who were recruited. The mules purchased goods with stolen funds, enabling cybercriminals to launder the money they acquired through malware attacks or other illegal means.

Source: United States

Digital Money and Virtual Currency Networks

PMLs also arrange schemes that allow criminals to cash out proceeds generated in virtual currency via online illicit markets (e.g. Dark Web drug-trafficking marketplaces). In many cases, payments for illicit drugs purchased online are transferred to e-wallets held in fiat currency or in virtual currency (e.g. Bitcoin). Afterwards, virtual currency is transferred through a complex chain of e-wallets, which may include the use of mixers and tumblers to further enhance the anonymity of the virtual currency transactions. Funds are then sent back to the e-wallet of the OCG, and subsequently transferred to bank cards and withdrawn in cash.

Financial instruments are issued under the names of money mules (usually students who obtain a bank card and then sell the bank card to criminals for a fee, knowing nothing about its subsequent usage and associated criminal activities). Money mules employed by the PML conduct ATM withdrawals in a coordinated manner, and then give the money to members of the client OCGs.

There are cases when the same financial scheme and the network of individuals worked for the benefit of multiple OCGs operating on the Dark Web. These persons then re-distributed funds to the respective OCGs.

Box 6. Laundering Proceeds from Dark Web Drug Stores

The Russian Ministry of Internal Affairs and FIU conducted an investigation into OCGs that sold drugs via the Dark Web. Customers could choose two ways to pay and transfer funds for their order either by an indicated e-wallet, held in fiat currency, or to a Bitcoin address. The majority of clients preferred using e-wallets held in fiat currency, instead of Bitcoins.

The financial scheme for the drug stores was arranged and managed by a financier and his network. The ML network was responsible solely for moving funds and had no links to drug trafficking. Numerous e-wallets and debit cards were registered in the names of front men. This usually involved students who issued e-wallets and credit cards, and then sold them to members of the ML network, unaware of the criminal purpose of their further usage. Some e-wallets were used at the placement stage of the laundering process and had a limit of USD 300 000, while other e-wallets had a higher limit.

To simplify the ML process, the network's IT specialists developed a 'transit-panel' that had a user-friendly interface and was accessible via the TOR browser. The transit panel automatically switched between e-wallets that were used for drug payments. Digital money was automatically moved through a complex chain of different e-wallets.

Money from e-wallets was then transferred to debit cards and withdrawn in cash via ATMs. Withdrawals via ATMs were conducted by "cash co-ordinators" who had multiple debit cards at hand (all cards were issued on the names of straw men[1]). Afterwards, cash was handed over to interested parties. In order to increase the complexity, proceeds were re-deposited on a new set of debit cards and transferred to the OCGs (usually located abroad).

In similar schemes, funds from e-wallets were exchanged into Bitcoins via virtual currency exchangers. The Bitcoins were used to pay salaries to members of the drug trafficking organisation. This included low-level members, such as small dealers and runners who facilitated the sale of drugs. The same financier worked with multiple owners of the Dark Web stores, distributing the laundered funds to the respective OCGs.

Note: 1. The term "straw men" refers to informal nominee shareholders and directors who are being controlled by the actual owner or controller of the company.

Source: The Russian Federation

Proxy Networks

Proxy networks are PMLs who supply a type of banking service to OCGs, generally through the use of multi-layered transfers via bank accounts. These specialised services offer all of the advantages that come with moving funds globally via the legitimate financial sector. The main task of these proxy networks is to move client funds to the final, pre-determined destination and to obfuscate the trail of the financial flows. In many cases, these schemes are supported by TBML mechanisms.

PML schemes that are arranged with the use of bank accounts consist of multiple layers of shell companies in different jurisdictions, which have been established purely to redistribute and mix funds from various sources. These shell companies could be located in the country where the predicate offence occurred, transit countries or countries where the final investment of funds is conducted. This scheme is designed to make the portion of funds that belong to a client untraceable. In most cases, laundered funds are transferred to a client's personal bank account(s), affiliated companies or foundations under their control, or handed over to them as physical cash.

In general, a cross-border ML scheme arranged by a proxy network has the following structure:

- **Step 1:** Clients' funds are transferred to accounts opened in the name of shell companies controlled by the PML, often through the use of legal entities controlled by them, or entities operating on their behalf. If the criminal proceeds were obtained in cash, controllers arrange to collect and deposit the cash into the accounts of PML-controlled shell companies.

- **Step 2:** Funds are moved through a complex chain of accounts established by domestic shell companies under fictitious contracts. The funds from different clients are mixed within the same accounts, which makes it difficult for investigators to trace the funds coming from a particular client.

- **Step 3:** Funds are transferred abroad under fictitious trade contracts, loan agreements, securities purchase agreements, etc. In most cases, accounts of the first-level layer of foreign companies are controlled by the same money launderers, who facilitated Step 1, or by foreign PMLs who act in collaboration with the domestic money launderers.

- **Step 4:** Funds are moved through a complex chain of international transfers. The ML infrastructure used (i.e. accounts set up by shell companies) is typically used to channel money that comes from all over the world. These

international money transfers often demonstrate similar geographical patterns.

- **Step 5:** Funds are returned to the accounts controlled by the initial clients, their close associates or affiliated legal entities and arrangements. Alternatively, the PML will purchase goods and services on behalf of the OCG. PMLs that arrange these schemes provide different reasons to justify or legitimise the wire transfers they conduct. These may include trade in various goods and services, import/export services, loans, consultancy services or investments. PMLs look for loopholes and other possible purposes for payments that give the veneer of legitimacy to these transactions. Bank accounts are chosen to make the activity appear legitimate, and to avoid suspicious transactions reporting and/or instances where the transaction are blocked by financial institutions. For example, PMLs use accounts of various characteristics (i.e. accounts where the activity volume was small, medium or large), in accordance with the sums laundered.

Box 7. Facilitating the Laundering of Proceeds from Bank Fraud

In 2015, Russian law enforcement authorities, in co-operation with the FIU and the Central Bank, disrupted a large-scale scheme to embezzle funds and subsequently conduct illicit cross-border transfers.

During the course of the investigation, it was established that OCG members assisted in stealing assets from a number of Russian banks. Typically, the bank management team knowingly granted non-refundable loans and conducted fictitious real estate deals, which led to the bank's premediated bankruptcy. Illicit proceeds were then moved abroad via accounts of shell companies.

Law enforcement authorities and the FIU, in co-operation with foreign counterparts, detected a wider scheme of illicit cross-border money transfers that was used to move proceeds from several predicate offences abroad. Funds were moved via accounts of domestic shell companies and offshore companies (registered in the UK, New Zealand, Belize and other jurisdictions), with their accounts held by banks in Moldova and Latvia, under the pretext of fictitious contracts and falsified court decisions.

One of the major launderers of this scheme received profits for his services in his own personal bank accounts from two offshore companies that were used in the scheme.

The OCG consisted of more than 500 members. Law enforcement authorities seized more than 200 electronic keys of online bank accounts; more than 500 stamps of legal entities; shadow accountancy documents, copies of fictitious contacts; and cash. Bank managers and other complicit individuals were arrested.

Source: The Russian Federation

Social engineering frauds and other types of Internet-based fraud are often a source of illicit proceeds that may be laundered through a proxy network:

Box 8. Creating Infrastructure to Launder Funds

This investigation was conducted by a specially designated Israeli Task Force for PML investigations, which includes members from the Israeli Police, Tax Authority, IMPA (FIU) and Prosecution. The investigation also involved the co-operation of LEAs in another country.

The suspects of the investigation were criminals conducting massive fraud and extortion, as well as PMLs, who assisted the predicate offenders in laundering the proceeds of crimes. Funds were laundered using shell companies established in Europe and the Far East. "Straw men," couriers and hawala-type services. The companies were established in advance in countries that were less susceptible for illegal activity in the eyes of the fraud victims.

The PML built the infrastructure that enabled the ML activity, which in turn was part of a global ML network. The PML, through the use of other individuals, opened foreign bank accounts, established foreign companies, and also used a repatriation network of foreign immigrants to move funds as part of the ML network.

The suspects transferred fraudulent proceeds to bank accounts opened in the name of the shell companies and straw men. The funds were then transferred to other bank accounts in the Far East and immediately the suspects withdrew money in cash by using couriers, hawala networks and MVTS providers in Israel to transfer the funds to their final destinations.

During the investigation, an Israeli suspect (one of the PMLs) was arrested by an LEA of a third country. This assisted the investigation in understanding the modus operandi of the PMLN. It was established that the PML of the network was also able to provide bank accounts of various characteristics (i.e. accounts where the activity volume was small, medium or large in accordance with the sums laundered). The bank accounts were thus chosen to make the activity look legitimate, avoiding unusual activity reports and/or instances where the transaction is blocked by the financial institution concerned.

Source: Israel

Proxy networks that facilitate cross-border movement of funds often tie into a wider network of other PMLs in several countries for the purpose of moving and laundering funds to and from the country where the predicate offence took place. PMLs who facilitate the outgoing flow of funds from the country where the predicate offence was conducted are typically part of a broader, global ML network that specialises in moving illicit proceeds around the globe. Some third-party money launderers, identified by responding countries, also acted through collaboration with other PMLs operating abroad which provided ML services at their request. The use of a global network of PMLs, located in different countries, as well as using different methods to transfer funds internationally, ensures the diversification of financial transactions and helps to limit the risk of detection. An analysis of proxy networks shows that PMLs may change their *modus operandi* and employ different contacts as needed.

Box 9. Large-Scale International Money Laundering Platform

A financial investigation was initiated into the embezzlement of public funds and suspected corruption, which led to the detection of a large-scale international ML platform that was used to move funds originating from different sources.

The proceeds of crime were moved to accounts of shell companies held with banks in Latvia, Cyprus and Estonia. The criminal proceeds were further transferred to accounts of companies controlled by the beneficiary's close associates and then moved back to Russia. Further investigation revealed that various companies used the same channel to move the funds.

A criminal proceeding on articles "Fraud", "Arrangement of organised criminal group" and "Money Laundering," according to the Criminal Code of the Russian Federation, was opened. The Central Bank of the Russian Federation withdrew the license of the Russian bank that facilitated frequent cross-border money transfers under fictitious contracts for violations of AML legislation. The European Central Bank also withdrew the license of a Latvian bank that facilitated the redistribution of criminal proceeds. A significant portion of funds was frozen on the accounts held by Latvian banks.

While the investigation of the case started with a particular predicate offence, it led to the identification of a wide international PML scheme that was used to move funds originating from various crimes. There are also indications that clients from other countries used this ML scheme. In a demonstration of the interconnectedness of PML, some companies involved in this scheme have financial links with a UAE company designated by the US in relation to the Altaf Khanani Money Laundering Organisation,[1] described in Box 1.

Note: 1. See Section III for the case study on this MLO.
Source: The Russian Federation

PML schemes and infrastructure can also be used to launder funds and to facilitate large-scale tax evasion schemes. In such schemes, multiple layers of shell companies may be used between the importer and producer of goods that are located abroad. Funds used for the purchase of foreign goods thus go through a complex chain of transactions, with only one portion of these funds used for the import deal. The rest is directed to accounts controlled by beneficiaries.

Proxy networks also use layering schemes to transform illicit proceeds generated within the financial system into cash. This is mostly arranged for those clients who need to move criminal proceeds from bank accounts to physical cash. The majority of such clients are involved in public funds embezzlement, tax fraud and cyber fraud schemes. At the final stage, funds are transferred to corporate bank cards, followed by subsequent cash withdrawals. The number of shell companies and personal bank accounts involved may exceed several thousands. This limits the risk of detection and diversifies possible losses.

In some cases, cash withdrawals may be conducted abroad. In one case, funds were channelled to accounts of companies registered in the Middle East, with subsequent

cash withdrawals via exchange houses. Cash was then transported back to the country of origin and declared on the border as profits from legitimate business activities in the Middle East, which were intended to be used for the purchase of real estate.

SECTION V: SUPPORTING MECHANISMS USED BY PROFESSIONAL MONEY LAUNDERERS

PMLNs use a wide variety of ML tools and techniques. Among the most significant mechanisms are TBML, account settlement mechanisms and underground banking.

Trade-Based Money Laundering (TBML)

TBML is defined as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origin."[3] There are various TBML variations that can be employed by PMLs. These include:

- *The purchase of high-value goods using the proceeds of crime*, followed by the shipment and re-sale of goods overseas;

- *The transfer of funds which purport to be related to trade*, or to the purchase of goods that are ultimately never shipped or received (also known as "phantom shipments");

- *Falsifying the number and/or value of goods being shipped* to be higher or lower than the corresponding payment, allowing for the transfer or receipt of the value of proceeds of crime (also known as over or under-invoicing);

- *Using the proceeds of crime to purchase goods for legitimate re-sale*, with payment for goods made to drug traffickers/distributors by legitimate business owners (e.g. the Black Market Peso Exchange - BMPE); and

- *Using Money (Peso) Brokers*, who are third parties that seek to purchase drug proceeds in the location where illicit proceeds are earned by drug cartels (e.g. Colombia, Mexico) at a discounted rate. Money brokers often employ many individuals responsible for collecting narcotics proceeds and disposing of those proceeds, as directed by either the drug trafficking organisation or the money brokers who serve as PMLOs.

Box 10. ML Network, Operating as a Trade-Based ML Scheme1

Project OROAD was a joint task force financial investigation, launched from a drug investigation into ML activities of a suspicious group[2]. Information received from FINTRAC helped identify a complex TBML where two of the group's central figures hired 10 nominees to establish 25 shell companies. The shell companies were opened using names across a diverse number of

---

[3] FATF, 2006.

industries: landscaping, interior design, electronics, metal recycling, plastics recycling, construction supplies, beauty supplies, etc.

The laundering network included legitimate businesses, operating in the financial and real estate sectors, as well as a small financial company, which was complicit in laundering the funds. The money launderer provided his accomplice at the financial company with large bags of cash, which were then deposited into business accounts in the name of shell companies. This continued until the accounts were closed by the financial institution that held the shell company's accounts, due to a high volume of suspicious transactions.

Investigators believe the ML group used a TBML scheme. The ML operation and the network of shell companies were largely centred on a logistics company. One of the money launderers was seen leaving the logistics company location with large bags of bulk cash, which were believed to be the proceeds of drug sales. The money launderer used nominees to make multiple cash deposits into their personal and business accounts.

The money launderer instructed nominees to either i) transfer funds back to the logistics company; or ii) transfer funds to other business accounts, held by nominees located in Canada, China, Panama and the US. Funds were sent by wire transfer, bank draft or cheque, some of which were then returned to the logistics company. In each case, the money launderer used fraudulent invoices to account for the proceeds of drug sales so that they could be more easily integrated into the financial system.

Investigators believe that some of the funds were transferred back to the Mexican drug trafficking organisation and to other companies controlled by the drug trafficking organisation in China, Mexico and the US. In some cases, funds were used for to purchase goods located in Panama or Mexico. The ringleaders in Canada established companies in these countries in attempts to make the transfers seem legitimate. The purchased goods were then shipped to other foreign countries for sale. Once the purchased goods arrive at the destination country, they were sold, and the proceeds of the sale (in the destination country's currency) were then transferred to the drug trafficking or ML organisation to provide the criminals with "clean" funds, laundered through TBML.

Notes:

1 See case study "Operation Snake" in Section III, which involves another professional ML network using a TBML and MVTS scheme

2 The investigation also revealed a number of bulk cash transactions between the ring and illegal money brokers; however, the focus here is on the ML ring.

Source: Canada

PMLs may also create and use false documentation, layer related financial transactions and establish shell and/or shelf companies to facilitate purported trade transactions. By using TBML mechanisms, PMLs can break the link between the predicate crime and related ML, making it difficult to associate the criminals with the ML activity.

Box 11. Venezuelan Currency Smuggling Network

During 2015, 10 limited liability companies established by a single person in Spain processed more than 110 000 transactions, totalling EUR 22.4 million, through mobile payment "point of sale (POS)" terminals. Nine of these companies were purportedly active as travel agencies, eight shared the same registered offices and six had the same associate and director.

The POS terminals held by these companies exclusively accepted payment cards issued by the Venezuelan government (Comisión de Administración de Divisas - CADIVI). Given strict currency controls in Venezuela, residents can only obtain foreign currencies when traveling abroad. Therefore, a maximum of USD 3 000 at a rate of 6.3 bolivars per dollar can be exchanged. This led to a large currency exchange fraud called "el raspao," where Venezuelan residents accessed euros or dollars, under the false pretence of a journey abroad. The payment cards issued by the CADIVI, at the official exchange rate, were debited abroad while drug traffickers received the counter value in cash, in euro or dollar notes, which was then smuggled back into Venezuela and sold on the black market at a rate of about ten times the official exchange rate. Authorities in Luxembourg suspect that the payment cards issued by CADIVI were smuggled in bundles to Spain and swiped through the POS terminals of complicit traders who operated through Spanish front companies.

Drug traffickers and Colombian cartels are believed to have taken advantage of this currency smuggling network in order to repatriate the proceeds generated in cash through drug sales in Europe back to South America. These criminals washed their illicit cash by handing it out to Venezuelan currency traffickers. Once processed, the debited amounts were credited to linked bank accounts. These bank accounts had International Bank Account Numbers (IBANs), issued by a former Luxembourg-licensed electronic money remitter.

AML investigations by the regulator and the financial intelligence unit (FIU) revealed that the Luxembourg electronic money remitter did not manage these accounts itself, as stipulated in regulation, but handed them over to a Bulgarian-licensed electronic money remitter, which used the accounts for its own customers. The POSs were sold to the Spanish front companies by the Bulgarian electronic money remitter. Additionally, the Spanish front companies applied for hundreds of withdrawal cards (most front companies had more than 10 withdrawal cards each), issued by the Bulgarian electronic money remitter, in order to allow them to withdraw cash from their accounts. About 106 000 withdrawals, totalling more than EUR 20 million were made at ATMs situated in Colombia. These withdrawals did not comply with the daily, weekly and monthly limits as laid out in the general terms and conditions of the Bulgarian electronic remitter. Authorities in Luxembourg were not aware of any related suspicious transaction reports that were reported to the Bulgarian FIU. The Luxembourg and Bulgarian electronic remitters were held by the same beneficial owner. Commissions received by the Bulgarian electronic remitter on the operations totalled as much as EUR 1.9 million, or 9 % of the amounts processed through the POSs.

Source: Luxembourg

Account Settlement Mechanisms

PMLNs can facilitate the settlement of accounts between multiple OCGs. They may do this for OCGs operating in different countries that generate proceeds from cash and hold funds within bank accounts. A PML may, for example, simultaneously provide ML services to criminals who have cash and want to send funds to bank accounts in other countries, and to criminals who have money in their bank accounts but need cash (e.g. to pay their networks and workers). This *modus operandi* is called an *account settlement mechanism*.

The case, below, illustrates how a PMLO accepted and moved cash by car to Belgium, as part of an account settlement mechanism.

Box 12. Money Laundering as Part of an "Account Settlement Scheme" Between Various Criminal Organisations

Several Belgian corporate customers transferred funds to the accounts of Belgian construction or industrial cleaning companies and their managers. These companies had a similar profile: they operated in the same industry, the managers were often from the same country, the articles of association were copied with slight modifications, and the companies' financial health was poor. Some companies had already gone bankrupt or no longer complied with their legal requirements.

Funds were channelled through different accounts: Part of the funds credited to the accounts was withdrawn in cash, presumably to pay workers. Another part of the funds were transferred to companies located abroad, in Europe and in Asia.

The funds transferred to Europe were credited to the accounts of other companies in the same industry. Often no explanation was provided for these transfers, even though the scale was significant. The references accompanying these transfers, if any, were vague. The majority of the funds were subsequently withdrawn in cash.

The funds transferred to Asia, mainly China and Hong Kong, were credited to the accounts of limited liability companies, which were not linked to the construction or industrial cleaning industry in any way.

Information received from a counterpart FIU revealed links with a criminal organisation involved in drug trafficking. This organisation, which held large amounts of cash, used an organisation that laundered the funds and transported the cash to Belgium by car. In Belgium, intermediaries then handed over the cash to various companies in Belgium that required cash to carry out their activities.

Based on this information, authorities have concluded that the Belgian construction and industrial cleaning companies involved in this case were part of an account settlement scheme. The cash proceeds of drug trafficking were used to pay illegal workers of Belgian companies.

Source: Belgium

Underground Banking and Alternative Banking Platforms

Underground banking is one tool often used by PMLs. This mechanism is used, with the goal of bypassing the regulated financial sector and creating a parallel system of moving and keeping records of transactions and accountancy.

Box 13. Investigation of Massive Underground Banking System

Subject X and his network of associates in British Columbia, Canada, are believed to have operated a PMLO that offered a number of crucial services to Transnational Criminal Organisations including Mexican Cartels, Asian OCGs, and Middle Eastern OCGs. It is estimated that they laundered over CAD 1 billion per year through an underground banking network, involving legal and illegal casinos, MVTSs and asset procurement. One portion of the ML networks illegal activities was the use of drug money, illegal gambling money and money derived from extortion to supply cash to Chinese gamblers in Canada.

Subject X allegedly helped ultra-wealthy gamblers move their money to Canada from China, which has restrictions on the outflow of fiat currency. The Chinese gamblers would transfer funds to accounts controlled by Subject X and his network in exchange for cash in Canada. However, funds were never actually transferred outside of China to Canada; rather, the value of funds was transferred through an Informal Value Transfer System. Subject X received a 3-5% commission on each transaction. Chinese gamblers were provided with a contact, either locally or prior to arriving, in Vancouver. The Chinese gamblers would phone the contact to schedule cash delivery, usually in the casino parking lot, which was then used to buy casino chips. Some gamblers would cash in their chips for a "B.C. casino cheque", which they could then deposit into a Canadian bank account. Some of these funds were used for real estate purchases. The cash given to the high-roller gamblers came from Company X, an unlicensed MVTS provider owned by Subject X. Investigators believe that gangsters or their couriers were delivering suitcases of cash to Company X, allegedly at an average rate of CAD 1.5 million a day. Surveillance identified links to 40 different organisations, including organised groups in Asia that dealt with cocaine, heroin and methamphetamine.

After cash was dropped off at Company X, funds were released offshore by Subject X or his network. Most transactions were held in cash and avoided the tracking that is typical for conventional banking. Subject X charged a 5% fee for the laundering and transfer service. As the ML operation grew, the money transfer abilities of Company X became increasingly sophisticated to the point where it could wire funds to Mexico and Peru, allowing drug dealers to buy narcotics without carrying cash outside Canada in order to cover up the international money transfers with fake trade invoices from China. Investigators have found evidence of over 600 bank accounts in China that were controlled or used by Company X. Chinese police have conducted their own investigation, labelling this as a massive underground banking system.

Source: Canada

An *alternative banking platform (ABP)* is an alternative bank that operates outside the regulated financial system. However, an ABP may use the facilities of the formal banking system, while creating a parallel accountancy and settlement system. ABPs are a form of shadow banking that make use of bespoke online software to provide banking services, without the regulated and audited customer due diligence checks. They are an effective way to transfer the ownership of money anonymously and provide banking services within a bank account across a number of individuals, without being reflected in traditional banking transactions. Usually, it is supported with special software that can encrypt traffic, manage transactions between accounts within the same platform, apply fees and assist with interaction with the outside financial system.

Box 14. Alternative Banking Platforms

An alternative banking platform (ABP) was used to assist organised crime groups (OCGs) in the UK to launder funds from VAT fraud. The ABP had a registered office in one jurisdiction with a holding company in a second jurisdiction and a bank account in a third jurisdiction. It was operated by a PMLN based in a fourth jurisdiction all outside of the UK. The ABP was used for a year with over EUR 400 million moved through it. The ABP was shut down and the creator of the financial software was arrested by international partners, with assistance from Her Majesty's Revenue and Customs (HMRC). The data gathered from the ABP servers was used to identify other ABPs and develop additional cases.

Source: United Kingdom

In some cases, PMLs use specialised software to create an ML scheme to move funds randomly through numerous accounts. This software is generally based on a random data generator principle.

SECTION VI: COMPLICIT/CRIMINAL FINANCIAL SERVICE PROVIDERS AND OTHER PROFESSIONALS

As mentioned in **Section II**, PMLs may occupy positions within the financial services industry (e.g. bankers and MVTS agents) and DNFBP sectors (e.g. lawyers, accountants and real estate professionals), and use their occupation, business infrastructure and knowledge to facilitate ML for criminal clients. The use of occupational professionals can provide a veneer of legitimacy to criminals and OCGs. As such, OCGs actively seek out insiders as potential accomplices to help launder illicit proceeds. In rare instances, complicit actors who facilitate PML schemes come from within a government institution (i.e. a corrupt official).

Box 15. Corrupt Official Joining Criminal Enterprise to Launder Funds

Ukraine's law enforcement and prosecution services conducted an investigation of a high-ranking official who abused his power and official position for approximately three years. The official agreed to participate in the

---

creation of a criminal organisation and implemented an illegal scheme for minimising tax liabilities, which led to the illegal use of a tax credit. The public official received a cash fee for his services, which were performed with the participation of other public officials and other members of the criminal organisation.

The public official conducted a number of functions to make illicit proceeds appear legitimate, including creating, registering and owning a number of shell companies on behalf of members of the criminal organisation and purchasing property on their behalf. The official also established offshore companies in Cyprus and the BVI using his relatives as nominees. The high-ranking official also acquired entities registered in Ukraine, which were controlled by his offshore companies, by transferring funds from a bank in Liechtenstein. Funds transferred into Ukraine were used to purchase property. Fictitious contacts or agreements (e.g. for consultation services) were also established using a network of fictitious entities for services that were never rendered.

Source: Ukraine

PMLs often ignore or circumvent AML/CFT requirements or actively conceal AML/CFT failures within a particular institution or business. They may also ignore professional obligations, such as restrictions associated with their licenses or professional ethics rules. While the exact definition of complicity is a matter of domestic law, it is widely understood as intentional acts carried out with knowledge or wilful blindness of the illicit nature of the funds with which the person is dealing. The ability of a criminal to purchase or gain ownership or control of a financial business is the ultimate measure of success.

Criminals will actively seek to recruit complicit insiders within existing institutions or businesses, since these individuals have insider access and may be able to falsify records or initiate transactions in a manner, which bypasses AML/CFT regulations or institutional practices. In rare circumstances, criminals may be able to compromise entire institutions or businesses, including by acquiring ownership or control of the institution and appointing their own criminal management. The complicit activity described above (insider compromise and institutional compromise) should not be confused with instances of lax compliance, weak internal controls or inadequate corporate governance structures, which can result in compliance deficiencies with AML/CFT requirements. A reputation for weak compliance, however, may make the institution more attractive for an OCG seeking out a corrupt insider.

Money Value Transfer Services (MVTS) Providers

Case studies and insight provided by delegations show that MVTS providers have knowingly facilitated PML activities, including currency conversions (i.e. foreign exchange), cash-based transactions, and/or electronic funds transfers. Complicit MVTS providers can play an important role in the placement stage of the ML process. The most common ML transactions facilitated by MVTS providers are:

- cash purchases of funds transfers at the physical location of MVTS providers;

- large cash deposits made in the accounts of individuals and businesses followed by a domestic transfer to the account of an MVTS provider, or the purchase of bank drafts (e.g. cashier's check) payable to an MVTS provider; and

- the purchase of bank drafts for the benefit of individuals and businesses, which are negotiated by MVTS providers to fund the purchase of funds transfers.

Box 16. Use of Foreign Exchange Broker and "Quick Drop" Facilities

A mechanic in the UK acted as a professional launderer for an unknown PMLN. The mechanic opened bank accounts in the UK, which were used to deposit GBP 5.3 million in cash between October 2013 and December 2014. Multiple deposits of GBP 25 000 were paid into the bank accounts per day using bank 'quick-drop' facilities. Once paid into the bank accounts, money was transferred to third-party bank accounts held in the UK and six other jurisdictions using bank and foreign exchange broker transfers. The mechanic was paid GBP 20 000 for moving the cash abroad. The launderer pleaded guilty to three charges of ML and, in April 2018, was sentenced to six years in jail and banned from being a company director for nine years.

Quick drop is a facility to deposit, cash either at the bank directly or at a third-party facility, where the money is counted and then transferred to the bank to be deposited[4]. Quick drop facilities allow cash to be deposited quicker, at more locations and often without coming into contact with staff.

Source: United Kingdom

Analysis conducted by some competent authorities indicates that complicit MVTS providers may continue to file suspicious transaction reports (STRs). For example, STRs may be filed so as not to arouse suspicion or give the perception that the MVTS provider is otherwise compliant. In jurisdictions that require other forms of transaction reporting, such as threshold cash transactions, complicit MVTS may operate two sets of account records (i.e. shadow accountancy), one of which is used exclusively for criminal clients and for which no reports are filed. Alternatively, these complicit MVTS providers may report the transactions using fictitious transaction details.

Box 17. Complicit MVTS Agents to Facilitate Third-Party ML

The Italian FIU identified a significant reduction in remittances sent to Country "A" within a three year period (from EUR 2.7 billion in 2012 to EUR 560 million in 2015). This data highlighted the specific exposure of this 'corridor' to the risk of channelling illegal funds.

Further analysis of STRs led to the detection of alternative channels, used by

---

[4] UK National Risk Assessment of Money Laundering and Terrorist Financing, October 2015

PMLNs, to transfer significant amounts to Country A. A significant portion of the reduction of remittances towards Country A was related to the migration of many Italian MVTS agents towards foreign ones that do not produce statistical reports under national legislations, and are not subject to Italian AML and fiscal requirements.

The FIU received many STRs concerning suspicious activity traced back to Italian money transfer agents. Financial flows were mainly characterised by significant cash deposits and wire transfers in favour of the Italian bank accounts of the foreign MVTS. Such financial flows allegedly referred to money remittances performed by MVTS agents. However, suspicion was triggered given that the agents sometimes deposited cash into their accounts through a branch of the bank located far away from their business. The FIU extended its studies to gain a better understanding of financial flows performed by the MVTS and agents, which revealed that in some cases:

- the MVTS legal representatives were involved;
- the MVTS had been recently incorporated;
- the MVTS had links to subjects originating from Country A;
- the MVTS had opened a branch in an Italian city that is well known for its growing economic and business links with Country A;
- many agents of the same foreign MVTS – all originating from Country A – had already been reported to the Italian FIU or had been prohibited from performing agent activities by the competent financial supervisory authority of Country A, for anomalous transactions and use of false ID documents for CDD purposes;
- the MVTS agents allowed their customers to structure transactions by splitting up remittances with several accomplices; and
- certain MVTS agents revealed tangible links to a common customer base.

In view of analysis carried out, the MVTS provider and agents were found to have disregarded AML obligations, exploiting asymmetries in the regulatory framework among different countries. A well-organised, skilled and complicit network of agents and foreign MVTS had been used to collect funds in Italy, and to transfer significant amounts abroad, splitting up remittances with several accomplices.

Source: Italy

Financial Institutions

The use of the international financial system has been instrumental in facilitating large-scale PML schemes. All of the complex layering schemes described in **Section IV** involve moving significant volumes of funds through various bank accounts in different jurisdictions opened on behalf of shell companies. These well-structured schemes often go undetected by banks, even in situations where there is an insider involved.

Investigative authorities have been able to detect patterns in how PMLs choose certain jurisdictions and banks that are used to move illicit proceeds. For example,

some criminals seek to use banks that operate in lax regulatory environments or have reputations for non-compliance with AML/CFT regulations.

It is challenging for competent authorities to establish factual evidence, which demonstrates that financial institutions are actively complicit in facilitating ML. Bank insiders generally do not communicate openly about their criminal conduct and may be able to leverage their insider status to conceal misdeeds. This can make it difficult to detect and prosecute wilful misconduct by complicit financial services professionals. A range of employees within financial institutions (from lower-level tellers to higher-level management) pose a significant vulnerability that can be exploited by money launderers, but also senior insiders who knowingly assist in ML may cause more damage.

Complicit bank employees may perform functions such as:

- Creating counterfeit checks;
- Monitoring (or not appropriately monitoring) money flows between accounts controlled by the co-conspirators;
- Co-ordinating financial transactions to avoid STR reporting;
- Accepting fictitious documents provided by clients as a basis for transactions, without asking any additional questions; and
- Performing 'virtual transactions' on the accounts of their clients – numerous transactions conducted, without an essential change of the net balance at the beginning and end of a working day.

Box 18. General Manager and Chairman of a Foreign Bank

An investigation by Italian authorities uncovered various ML operations that were carried out by senior foreign bank officials (general manager and chairman), together with a complicit accountant and a lawyer. The illicit proceeds were derived from an international cocaine trafficking organisation.

The criminals were put in contact with the general manager and the chairman of the foreign bank, which was experiencing a serious liquidity crisis at the time. The criminals and the bank executives agreed that one of the drug traffickers would deposit, in his own name, about EUR 15 million at the bank in crisis. This bank committed to provide the two professionals (the lawyer and accountant, noted above, who were also brothers) with a given amount of money in compensation for the intermediation work they performed, to be credited to accounts specifically opened in their names at the bank.

The accountant was also in charge of performing accounting tasks for several companies belonging to the drug trafficker. Following the intermediation activity, the bank's general manager received EUR 1.3 million, in two instalments, from a deposit made in the name of the drug trafficker. Subsequently, the bank's general manager, with the approval of the bank's chairman, started complex financial operations aimed at concealing the unlawful origin of the money deposited.

Authorities were able to ascertain the role played by the lawyer, leaving no

---

doubt as to his function as an intermediary between his client (custodian) and the bank, and the lawyer's knowledge of the actual illicit source of the money involved.

Source: Italy

The case below demonstrates a combination of different elements and tools, including the sale of shell companies, facilitation of transactions by complicit bank employees and the execution of deals on securities markets.

Box 19. Complicit Bank Employees, Securities Market Deals and the Sale of Shell Companies

An investigation by Russian authorities, conducted in co-operation with foreign FIUs, uncovered an ML and tax evasion scheme that was arranged by complicit bank employees and brokers.

Funds accumulated in bank accounts of shell companies were transferred abroad under the pretext of securities purchases by order of broker "R." At the same time, two broker companies operating on the London Stock Exchange sold shares for the same price, thus facilitating the transfer of money via mirror trading.

All limited liability companies used in this scheme were established by a legal service firm, specialising in the sale of "off-the-shelf" companies. Criminal proceedings were opened. The licenses of one of the banks that facilitated cross-border transfers, and of the securities company, were withdrawn for violations of the AML legislation.

Source: The Russian Federation

1.   The cases analysed and information received also demonstrated that private banking advisors may act as PMLs and provide services to conceal the nature, source, ownership and control of the funds in order to avoid scrutiny, by employing various techniques, including:

▪ Opening and transferring money to and from bank accounts held in the names of individuals or offshore entities, other than the true beneficial owners of the accounts;

▪ Making false statements on bank documents required by the bank to identify customers and disclose the true beneficial owners of the accounts;

▪ Using "consulting services" agreements and other similar types of contracts to create an appearance of legitimacy for illicit wire transfers;

▪ Maintaining and using multiple accounts at the same bank so that funds transfers between those accounts can be managed internally, without reliance on international clearing mechanisms that are more visible to law enforcement authorities; and

- Opening multiple bank accounts in the names of similarly-named companies at the same, or different, institutions so wires do not appear to be coming from third parties.

Legal and Professional Services

In order to place greater distance between their criminal activity and the movement of funds, some OCGs use the services of third-party money launderers, including professional gatekeepers, such as attorneys, accountants and trust and company service providers (TCSPs). One delegation noted that OCGs tend to use professional service providers to set up corporate structures, and that accountants are favoured due to the range of skills and services that they may provide. There are case examples demonstrating that these types of professionals have been recruited to work as PMLs on behalf of larger criminal enterprises, such as DTOs. FATF's 2013 Report on *ML and TF Vulnerabilities of Legal Professionals* mentions that criminals often seek out the involvement of legal professionals in their ML/TF activities because they may be required to complete certain transactions or provide access to specialised legal and notarial skills and services, both of which can assist the laundering of the proceeds of crime

---

Box 20. A Complicit Lawyer and Bank Employee

A lawyer in Texas was convicted for laundering money for an OCG and engaging in a variety of fraud schemes. The OCG operated in the US, Canada, Africa, Asia and Europe. A complicit bank employee was also convicted for her role in creating counterfeit checks and monitoring money flows between the numerous accounts controlled by the OCG.

All of the victims of these various fraud schemes were instructed to wire money into funnel accounts held by other co-conspirators (money mules), who then quickly transferred the money to other US accounts as well as accounts around the world before victims could discover the fraud. Several millions of dollars were laundered in this manner. The numerous bank accounts opened by the mules served as the initial "layer" in the laundering process, which allowed co-conspirators to distance or conceal the source and nature of the illicit proceeds. For example, during a one-year period, a key money mule opened 38 fraudulent bank accounts.

The fraud schemes took several forms. Many victims were law firms that were solicited online provided counterfeit cashier's checks for deposit into the firms' trust accounts. The law firms were then directed to wire money to third-party shell businesses controlled by the co-conspirators. The fraud conspiracy also employed hackers who compromised both individual and corporate e-mail accounts, ordering wire transfers from brokerage and business accounts to shell accounts controlled by co-conspirators. The shell companies were incorporated in Florida with fictitious names and then used to open bank accounts at banks in Florida in those names.

The licensed attorney in Texas worked for the co-conspirators by laundering victim money through an interest on lawyers trust account (IOLTA). He also

---

> met with individual money mules to retrieve cash from their funnel accounts. The lawyer recruited his paralegal and others to open accounts used in the laundering scheme.
>
> Source: United States

One case involves a licensed attorney who was considered a full member of an OGC. As in the case above, the attorney facilitated ML services by using his interest on lawyers trust account, or ILOTA[5], to transfer the proceeds of drug trafficking and fraud.

Box 21. Operation CICERO

This case was initiated by a special currency police unit within the Guardia di Finanza as a follow-up investigation to a judicially authorised search conducted on the boss of a major organised crime group (La Cosa Nostra or LCN) in Palermo, Italy. This investigation was aimed at identifying those individuals acting as nominees, as well as individuals who facilitated the movement of criminal proceeds on behalf of LCN. The investigation identified that a well-known lawyer was the beneficial owner of the companies used to launder funds via a Palermo-based construction company, which was linked to family members of the organised crime boss.

The lawyer performed a "money box" function for the LCN, which consisted of managing the financial resources of the crime group with the purpose of concealing the origins of the illicit proceeds and avoiding detection by authorities of any assets purchased from these proceeds. Through his professional relationships, the lawyer developed and tapped into an elite social network, which he also made available to the organised crime group.

The lawyer, who was operating as a PML, conducted a number of services, such as: (a) obtaining a mortgage to purchase an apartment with EUR 450 000 in criminal proceeds on behalf of an organised crime family member; (b) using a fictitious contract to purchase an apartment with EUR 110 000 on behalf of the organised crime group; and (c) layering and integrating legal funds with criminal assets derived from construction work carried out on land purchased with criminal proceeds.

This investigation led to confiscation proceedings against nine individuals totalling EUR 550 000 as well as seven properties owned by the lawyer.

Source: Italy

---

[5] An IOLTA is an account opened by an attorney with the intention of holding client funds for future services. It is opened at a bank with a presumed higher level of confidentiality accorded to attorney-client relationships and related transactions.

PMLs also often use shell companies to facilitate complex ML schemes. Professional services may be used, such as the services of a TCSP or a lawyer, when setting up a shell company. Such professionals can supply a full range of services, including the incorporation of the company, the provision of resident or nominee directors, and the facilitation of new bank accounts.

Box 22. Use of Shell Companies and Accountant Providing Corporate Secretarial Services

Person G was a chartered accountant in the business of providing corporate secretarial services to small and medium-sized enterprises. As part of these services, he incorporated companies on behalf of his clients and acted as the resident director of companies whose directors were not ordinarily residents in Singapore.

Persons N and S, members of a foreign syndicate, approached Person G to set up three companies, Company K, Company W and Company M, and to apply for their corporate bank accounts in Singapore. Once the accounts were set up, Persons N and S left Singapore and never returned. Person G was appointed the co-director of the three companies; although, he was neither a shareholder, nor the authorised bank signatory of these companies.

These companies received criminal proceeds in their bank accounts derived from various frauds amounting to over SGD 650 000. The funds were quickly transferred by Person S to overseas bank accounts.

The companies had committed the offence of transferring benefits of criminal conduct, attributable to Person G's neglect. There was a lack of supervision by Person G over the companies' affairs, which allowed the foreign syndicate to have unfettered control over the companies and partake in their ML activities unimpeded. In January 2016, G was convicted of ML offences and for failing to exercise reasonable diligence in discharging his duties as a director. He was sentenced to a total jail term of 12 months, fined SGD 50 000 and disqualified from acting as a company director for the five years following his sentence.

Source: Singapore

After opening bank accounts in the name of shell companies, professional launderers may operate these accounts from overseas, receiving criminal proceeds from different individuals and companies to layer funds. The funds received in the shell companies' accounts are usually transferred out of the jurisdiction within a few days.

TCSPs are often blind to what their clients actually use the companies for, and therefore do not consider themselves complicit in ML schemes. However, a number of case studies have demonstrated that some TCSPs market themselves as 'no questions asked,' or being immune from official inquires. Moreover, if the TCSP also acts as the director of the company, the TCSP has to perform these duties as a director and could be held liable for the offences committed by the company, as illustrated in the above case study.

Law enforcement agencies worldwide have noted that corporate structures are often used in PML schemes and that professional service providers are used in setting up structures. Law enforcement agencies have identified the use of complex corporate structures and offshore vehicles to conceal the ownership and facilitate the movement of criminal proceeds and that PMLNs exploit some TSCP services in the creation of structures. A handful of current investigations across the globe have indicated that TCSPs act as nominee directors of corporate structures with similar behaviours, observed whether large corporates or smaller TCSPs, including:

- using a 'tick the box' approach for compliance activity;

- distancing themselves from risk (i.e. downplay their responsibility);

- utilising chains of formation agents in multiple jurisdictions;

- engaging in deliberately negligent behaviour; and

- forging signatures and fraudulently notarising documents.

Box 23. Money Laundering through Real Estate Investments, Gastronomic Services and Show Production Services Linked With Drug Trafficking

An investigation was triggered by information received from OFAC, which revealed that an illicit network was conducting business activities in Argentina. This network was linked to an individual, J.B.P.C., who was suspected of being a member of a criminal organisation.

J.B.P.C., his family and business partners were also shareholders in a number of companies around the globe. More specifically, three Argentine companies (two operating companies and a management company) were suspected of developing ambitious real estate projects across the country. The president and main shareholder of those companies was Mr. B, a lawyer and friend of J.B.P.C. This person provided knowledge and experience on how to develop the businesses. Additional analysis revealed that J.B.P.C. was the shareholder of two other companies, which appeared as owners of the land where major real estate developments were to be undertaken.

Tax information that was collected by authorities revealed that these companies received accounting advice from Mr. C, who was a chartered accountant. He was also a shareholder and member of the Board of Directors of the concerned companies. Other transactions from J.B.P.C. were also detected during the same period. They were linked to two additional Argentine companies that provided bar services, coffee services and show production services. For one of the OFAC listed companies, it was discovered that the stock of the company was owned in its entirety by J.B.P.C.'s closest relatives. Likewise, management positions were occupied by his partners and close relatives. Another company, also with ties to J.B.P.C., opened an office in Argentina with the help of another lawyer, Mr. D.

The investigation into this case was conducted by FIU-Argentina in co-ordination with other domestic LEAs, as well as foreign counterparts in

Colombia (FIU-Colombia) and the United States (OFAC and DEA). Strong international co-operation was crucial to the success of this investigation, and joint efforts led to a significant number of simultaneous searches in Argentina, as well as in the other foreign jurisdiction where J.B.P.C. ran a majority of his illegal business. As a result, J.B.P.C., Mr. B and his spouse, Mr. C and Mr. D were arrested. Their property was also seized. Currently, they are facing prosecution in Argentina.

Source: Argentina

Payment Processing Companies

Payment processing companies provide payment services to merchants and other business entities, such as credit card processing or payroll processing services. Typically, bank accounts held by payment processors are used to facilitate payments on behalf of their clients. In certain circumstances, payment processing companies essentially act as "flow-through" accounts – there is no requirement for them to divulge the identities of their individual clients to financial institutions. Traditionally, payment processing companies were established to process credit card transactions for conventional retail outlets. However, over time, payment processing companies have evolved to serve a variety of domestic and international merchants, including Internet-based and conventional retail merchants, Internet gaming enterprises and telemarketing companies.

Payment processing companies can be used by criminal organisations to mask transactions and launder the proceeds of crime. For example, payment processing companies have been used to place illicit proceeds that originated from foreign sources directly into financial institutions[6].

A number of countries have observed the use of payment processing companies by suspected ML networks. In other instances, telemarketing companies have also been suspected of providing payment processing services, where illicit proceeds are co-mingled with payments suspected of being related to mass marketing fraud. Authorities suspect that these types of payment processors may be used by members and associates of multiple transnational OCGs.

Box 24. International Payment Processor Providing ML Services

PacNet, an international payment processor and MVTS provider based in Vancouver, Canada, helped dozens of fraudsters gain access to US banks. PacNet has a 20-year history of engaging in ML and mail fraud, by knowingly processing payments on behalf of a wide range of mail fraud schemes that target victims throughout the world. When it was shut down, PacNet consisted of 12 individuals and 24 entities across 18 countries. The network collectively has defrauded millions of vulnerable victims across the US out of hundreds of

---

[6] FINCEN, 2012 and FFIEC, nd.

millions of dollars.

With operations in Canada, Ireland and the UK, and subsidiaries or affiliates in 15 other countries, PacNet was the third-party payment processor of choice for perpetrators of a wide range of mail fraud schemes. US consumers receive tens of thousands of fraudulent lottery and other mail fraud solicitations nearly every day that contain misrepresentations designed to victimise the elderly or otherwise vulnerable individuals.

PacNet's processing operations helped to obscure the nature of the illicit funds and prevented the detection of fraudulent schemes. In a typical scenario, scammers mailed fraudulent solicitations to victims and then arranged to have victims' payments (both checks and cash) sent directly, or through a partner company, to PacNet's processing operations. Victims' money, minus PacNet's fees and commission, were made available to the scammers through wire transfers from the PacNet holding account, as well as by PacNet making payments on behalf of the scammers, thereby obscuring the link to the scammers. This process aimed to minimise the chance that financial institutions would detect the scammers and determine their activity to be suspicious.

The mail schemes involved a complicated web of actors located across the world and each scheme followed a similar pattern. These schemes involve a consortium of entities, including direct mailers, list brokers, printer/distributors, mailing houses, "caging" services[7], and payment processors. These six diverse groups worked together to (i) mail millions of solicitation packets each year, (ii) collect and distribute tens of millions of dollars in annual victim payments, and (iii) attempt to obscure their true identities from victims and law enforcement agencies worldwide.

Source: United States

Virtual Currency Payment Products and Services (VCPPS)

As noted in **Section IV**, PMLs offer a variety of services including the use of virtual currency in an attempt to anonymise those committing crimes and their illicit transactions. The use of complex, computer-based fraud schemes has led cyber criminals to create large-scale mechanisms to move the proceeds earned from these schemes. More specifically, virtual currency exchangers have been used as unlicensed or unregistered MVTS providers to exchange criminal proceeds in the form of virtual currency to fiat currency. In 2015, FATF issued guidance to demonstrate how specific FATF Recommendations should apply to convertible virtual currency exchangers in the context of VCPPS, and identify AML/CFT

---

[7] The processing of responses to direct mail is often conducted by a third party hired to perform various services, which may include processing payments, compiling product orders, correcting recipient addresses, processing returned mail, providing lockbox services, and depositing funds and the associated data processing for each of these services. Caging is a shorthand term for the service bundle.

measures that could be required[8]. Case studies have nonetheless shown that complicit virtual currency exchangers, which have been intentionally created, structured, and openly promoted as criminal business ventures, are being used.

Digital payment systems can also facilitate other crimes, including computer hacking and ransomware, fraud, identity theft, tax refund fraud schemes, public corruption and drug trafficking. Complicit virtual currency providers also utilise shell companies and affiliate entities that cater to an online, worldwide customer base to electronically transfer fiat currency into, and out of, these exchangers (effectively serving as electronic money mules). Users of these complicit services have openly and explicitly discussed criminal activity on these providers' chat functions, and their customer service representatives have offered advice on how to process and access money obtained from illegal drug sales on Dark Web markets.

Box 25. Complicit Virtual Currency Exchanger

On July 26, 2017, a grand jury in the Northern District of California indicted a Russian national and an organisation that he allegedly operated, BTC-e, for operating an unlicensed money services business, ML and related crimes. The indictment alleges that BTC-e was an international ML scheme that allegedly catered to criminals, particularly cyber criminals, and evolved into one of the principal means by which criminals around the world laundered the proceeds of their illicit activity. The indictment alleges that one of the operators of BTC-e who directed and supervised BTC-e's operations and finances, along with others, intentionally created, structured, operated and openly promoted BTC-e as a criminal business venture, developing a customer base for BTC-e that was heavily reliant on criminals. BTC-e was also one of the world's largest and most widely used digital currency exchangers. The investigation has revealed that BTC-e received more than USD 4 billion worth of virtual currency over the course of its operations. In addition to the indictment charging BTC-e and one of its operators with the violations noted above, FinCEN – in close co-ordination with the Justice Department – assessed a USD 110 million civil money penalty against BTC-e for wilfully violating US. anti-money-laundering laws.

Source: United States

SECTION VII: CONCLUDING REMARKS

This threat report addresses criminal actors, including organised crime groups that specialise in the provision of professional money laundering services and complicit actors who are knowingly involved, or are deliberately negligent, in the laundering process. A number of characteristics have been identified, based on an extensive case review (including, the role and functions of PMLs; the business models used; and relevant typologies and schemes). A non-public version of the report is available to Members of the FATF and the FATF Global Network upon request. This non-

---

[8] FATF, 2015.

public version includes further information, such as practical recommendations for the detection, investigation, prosecution and prevention of ML.

REFERENCES

FATF (2006), *Trade-Based Money Laundering*, FATF, Paris, France,
www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html

FATF (2012a), *FATF Recommendations*, FATF, Paris, France,
www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

FATF (2012b), *FATF Guidance on Financial Investigations*, FATF, Paris, France,
www.fatf-gafi.org/publications/methodsandtrends/documents/operationalissues-financialinvestigationsguidance.html

FATF (2013a), *FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems – FATF Methodology*,
FATF, Paris, France,
www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html

FATF (2013b), *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals,* FATF, Paris, France,
www.fatf-gafi.org/publications/methodsandtrends/documents/mltf-vulnerabilities-legal-professionals.html

FATF (2015), *Guidance for a Risk Based Approach to Regulating Virtual Currency*,
FATF, Paris, France
www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

FATF – Egmont Group (2018), Concealment of Beneficial Ownership, FATF, Paris, France,
www.fatf-gafi.org/publications/methodsandtrends/documents/concealment-beneficial-ownership.html

FFIEC (nd), Bank *Secrecy Act, Anti-Money Laundering Examination Manual, Third-Party Payment Processors—Overview,* Bank Secrecy Act/Anti-Money Laundering InfoBase, Federal Financial Institutions Examination Council:
www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_063.htm

FINCEN (2012), *Risk Associated with Third-Party Payment Processors,* FIN-2012-A010. October 22, 2012, Department of the Treasury – Financial Crimes Enforcement Network, Washington, United States, October 22, 2012,
https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A010.pdf

www.fatf-gafi.org

July 2018

Professional Money Laundering

Professional money launderers (PMLs) provide services to criminals and organised criminal groups by laundering the proceeds of their illegal activities. They may provide the entire infrastructure for complex ML schemes (e.g. a 'full service') or construct a unique scheme tailored to the specific needs of a client that wishes to launder the proceeds of crime. This report identifies the specialist skill sets that PMLs offer their clients in order to hide or move their proceeds, and provides a detailed explanation of the roles performed by PMLs to enable authorities to identify and understand how they operate. This report also provides recent examples of financial enterprises that have been acquired by criminal enterprises or co-opted to facilitate ML.

This report aims to assist authorities to target PMLs, as well as the structures that they utilise to launder funds, in order to disrupt and dismantle the groups that are involved in proceeds-generating illicit activity so that crime does not pay.