



# **EGMONT GROUP BULLETIN**

## **Professional Money Laundering Facilitators**

Information Exchange Working Group

# IEWWG

July 2019  
-Public version-

## THE EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS

### PUBLIC BULLETIN: BUSINESS E-MAIL COMPROMISE FRAUD

*This Bulletin should assist authorities and reporting entities in better detecting, investigating, and reporting the proceeds of professional money laundering activities.*

*The Egmont Group is a united body of 164 Financial Intelligence Units (FIUs). The Egmont Group provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing (ML/TF).*

For more information on Egmont Group, please visit our website: [www.egmontgroup.org](http://www.egmontgroup.org)

### BULLETIN ON PROFESSIONAL MONEY LAUNDERING NETWORKS

Identification number: EG-Bulletin-02/2019

Date: June 30, 2019

Intended Recipients: Financial Intelligence Units, Law Enforcement Authorities, Reporting Entities.

#### DEFINITIONS<sup>1</sup>

**Professional money laundering** is a subset of third-party ML. **The main characteristic that makes PML unique is the provision of ML services in exchange for a commission, fee or other type of profit.**

PMLs can belong to three categories: (i) individuals, (ii) organisations or (iii) networks:

An **individual PML** 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).

A **Professional Money Laundering Organisation (PMLO)** 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.

A **Professional Money Laundering Network (PMLN)** 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

---

<sup>1</sup> The following report served as a basis for the current analysis: FATF (2018), *Professional Money Laundering*, FATF, Paris, France, <http://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf>

range of ML services. These interpersonal relationships are not always organised and are often flexible 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:

- a the reputation of the individual PML;
- b the total amount of funds being laundered;
- c the denomination (i.e. value) of the banknotes (in cases involving cash);
- d 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
- e 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 be done 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 via 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.

### ROLES AND FUNCTIONS

Numerous roles and functions are performed by PMLs. 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 relevant players and ensure that all relevant aspects of PMLs are detected, disrupted and ultimately dismantled.

1. **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.
2. **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.
3. **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/passwords, and buy SIM-cards for mobile communication.
4. 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 can be done either as a fee for their money transfer services or as a one-time payment for their services.
5. **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.
6. **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.
7. **Investing or purchasing assets:** Where needed, real estate or other assets such as precious gems, art or luxury goods and vehicles 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.
8. **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).

9. **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

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

### **Stage I: 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, 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 II: 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 the professional launderer 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. 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 III: 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.

**RECOMMENDED RED FLAG INDICATORS FOR FIUS AND PRIVATE SECTOR**

- Financial transactions via different bank accounts are managed from the same set of IP addresses;
- Different geographic locations of companies, banks accounts, owners and managing directors, while the same IP addresses are used for online account management;
- Individual or single entity opening or managing numerous bank accounts in a coordinated fashion;
- Transit movement of funds through bank accounts of companies (accounts of companies are used to receive and immediately transfer money, and the account balance by the close of the day is zero).
- No tax, insurance or social payments are conducted by companies that are used for the transit movement of funds;
- Regular cross-border transfers of funds via accounts of shell companies related to loan agreements and payments for services;
- Transferring funds abroad to buy goods that are never shipped, received or documented;
- Payments for real estate and other high-value assets are performed by offshore companies;
- Payments for goods delivered to third countries are performed by offshore companies that are not parties to contract;
- Bank accounts in one jurisdiction, held by corporate structures in a second jurisdiction with beneficial owners in a third jurisdiction, are used to pay or receive transactions for goods or services where they are unconnected to the businesses sending or receiving the transaction, or the trade the transaction is for;
- A significant number of STRs/SARs regarding legal entities registered via the same TCSP or having the same nominal shareholders and directors;
- Cash withdrawals or cash deposits from or to multiple bank cards are conducted systematically via the same ATMs (very small intervals between cash withdrawal or deposit transactions with different cards indicate that these transactions are managed by the same person);
- Participating companies are registered at one or more “virtual” addresses, at addresses of mailboxes using special services providers (advocates, lawyers and other).