Strategic Analysis on Professional Money Laundering (PML) and Foreign Proceeds of Crimes

UAE-FIU 2021

UAE Financial Intelligence Unit – P.O.Box 854, Al Karamah Street – International Tower, Abu Dhabi.

Phone No: +97126919955

Email address: uaefiu@uaefiu.gov.ae

List of Acronyms

Terms & Definitions	Description
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
CBUAE	Central Bank of the UAE
FATF	Financial Action Task Force
FI	Financial Institution
GoAML	The Financial Intelligence Unit online reporting application
LEA	Law Enforcement Authority
PML	Professional Money Laundering
RFI	Request for Information
SAR	Suspicious Activity Report
SD	Spontaneous Dissemination
STR	Suspicious Transaction Report
UAE FIU	Financial Intelligence Unit of the UAE

Content and objectives

This Guidance is part of the Strategic Analysis Plan (SAP) adopted by the UAE-FIU also considering the requirements of the *National Assessment of Inherent Money Laundering and Terrorist Financing Risks in the United Arab Emirates* (NRA) and the following *UAE National Action Plan to Implement the Combating Anti-Money Laundering and Terrorism Financing National Strategy 2020-2023* (NAP).

This report is based on the results of the strategic analysis of available data relating to **Professional Money Laundering (PML) and the Foreign Proceeds of Crimes**.

The purpose of this Guidance is to:

- Promote awareness on the characteristics of Professional Money Laundering (PML);
- Identify relevant PML trend and/or typology;
- and to develop a list of indicators as a guidance to Reporting Entities on possible PML activities.

Methodology, Sources and Timeline

This report is based on the strategic analysis of data and information held by the UAE-FIU, as well as data and information obtained from the Reporting Entities "REs", particularly in the period January 2020 to June 2021.[1]

[1] The data and information analyzed include but are not limited to STRs and SARs databases; Cash declarations; information received from Counterpart FIUs, information received from REs.

I. Introduction

Professional Money Laundering (PML) is known as the facilitating of money laundering services on behalf of criminals or criminal groups for a fee. PML is offered/conducted by professionals (Professional Money Launders 'PMLs') either as individuals or in a form of group or even a network and usually engage in a sophisticated money laundering schemes to enable criminals to evade Anti-Money laundering and counter terrorist financing measures. PML Clients generally are not distinguished between drug dealers, fraudsters, human traffickers, or any other criminal with a need to move or conceal unlawful gains. These are all potential PML Clients, including single natural persons or legal entities, or even Organized Criminal Groups (OCGs).

Though PMLs facilitate Money Laundering using their wide expertise, specialized services and business modules, they are not necessarily directly involved in the commission of criminal activities, which initially generated the illicit proceeds, however, they are still considered as criminals. PMLs usually operate in a large scale that could also be a subset of Third-Party Launderers. From the analysis of this project, the extent to which those so-called intermediaries or launderers are involved or/and recruited cannot be determined.

The Financial Action Task Force (FATF) report on Professional Money Laundering (July 2018) [2], divided PMLs into three categories;

1. **Individual** such as, accountants, legal advisors, lawyers, bankers, agents or presenters specialized in company formation and legal arrangements.
2. **Professional Money Laundering Organization (PMLO)** is when two or more individuals forming a structured group facilitating the laundering of illegal proceeds.
3. **Professional Money Laundering network (PMLN)** usually operate in a larger scale and involve foreign jurisdictions. They may also include individual PMLs as well as PMLOs. This complex scheme is very hard to be detected by Law Enforcement Authorities.

During this analysis, the UAE-FIU has identified some common techniques of PML linked with specific high-risk sectors, professions, or activities, for example, Trade Based Money Laundering (TBML), Money Services Business (MSBs), Designated Non-Financial Businesses and Professions (DNFBPs), the abuse of Legal Entities, and Virtual Currencies. Some of the common tools that PMLs tend to use is Shell or Front Companies, and Money Mules.

[2] FATF report on PML – July 2018.

The analysis of this project also presumed that not all criminals have a tendency to use PMLs to get a veneer of legitimacy on their illicit proceeds, some of them would launder the funds by themselves through typical Money Laundering stages - Placement, Layering, Integration. However, PML service can be sought for more sophisticated Money Laundering schemes.

PMLs were found also similar to 'Illegal Hawala' providers in a way that they both use "Shadow Accountancy" in record keeping, in which a hidden set of financial book or ledger account containing details of transactions as well as their clients' (criminals for whom they launder the funds) details. The aim of this is to hide the identity of criminals and harden the trace of illicit funds for Law Enforcement Authorities.

This report describes later the main PML trends and techniques identified during this analysis, and exemplifies sanitized cases illustrating some relevant schemes of PML identified and demonstrating the level of awareness of Reporting Entities in the UAE.

II. Overview of Relevant Data and Information underlying the Strategic Analysis

The analysis presented in this report are based on a broad range of data and information, including, but not limited to, the databases directly accessible by the UAE-FIU particularly the **Suspicious Transaction Reports (STRs)** and **Suspicious Activity Reports (SARs)** database (GoAML). The data and information received from UAE Authorities - such as the Federal Public Prosecution and Local Police Departments, and the Federal Customs Authority (FCA) - and counterpart Financial Intelligence Units (FIUs), particularly in the period 2020-2021 (June).

The UAE-FIU analyzed all the available and obtainable data and information to assess the current level of understanding related to PML, and to identify relevant trends and typologies, furthermore, to develop a list of Red Flags/Indicators to assist Reporting Entities and other relevant Stakeholders identify potential PML activities.

› **Intelligence Reports and Requests received by UAE-FIU**

A review on a sample of around **300 Suspicious Transaction Reports (STRs)/ Suspicious Activity Reports (SARs)** received from reporting entities and more than **300 international requests** such as **Inward Request for Information (IRIs)** and **Inward Spontaneous Dissemination (ISDs)** received from counterpart FIUs was conducted in this report. The review of the said data was vital in order to assess the vulnerabilities of the UAE's

financial system in relation to identification of PML-related techniques and activities conducted to launder foreign proceeds of crime.

From the review, it was observed that the most common techniques used by criminals to route illicit funds to UAE was through the following:

- Establishment of Legal Entities with simple or complex structure
- Purchase of assets, mainly real estate
- Trade-based activities

On the other hand, from the intelligence reports received from counterpart FIUs, it was perceived that PML clients (criminals) were possibly linked with the following predicate offences identified by counterpart FIUs:

- Corruption and bribery
- Embezzlement
- Drug Trafficking and Human Trafficking
- Smuggling (Gold and/or Foreign Currencies)
- Fraud

Further to the above, the UAE-FIU identified a possible connection between Politically Exposed Persons (PEPs) and PML. Corrupted PEPs have a higher tendency in using PMLs, since in several requests, there are high-ranking public officials and company executives involved who had originally perpetrated fraud, embezzlement, corruption or bribery in their home countries and siphoned off the illegally obtained funds to the UAE.

› **Analysis of FCA Data and Requests received from other Local Authorities**

The analysis of this project also presumed that not all criminals have a tendency to use PMLs to get a veneer of legitimacy on their illicit proceeds, some of them would launder the funds by themselves through typical Money Laundering stages - Placement, Layering, Integration. However, PML service can be sought for more sophisticated Money Laundering schemes that usually involve aforementioned predicate offenses and international organized groups or networks that operates in multiple jurisdictions.

From the analysis of FCA data, alongside other information received by the UAE-FIU, it was observed that Organized Crime Groups use 'Money Mule Networks'. Involving individuals or groups arriving to the UAE carrying large cash from various jurisdictions. The cash is declared to the local customs authority in favor of a Legal Entity or an Exchange House, or in some instances declared as for Trading purposes. (*Please see the next section 'Trends and Typologies'*).

III. Trends and Typologies

Underlying the analysis of this project, in an attempt to identify and determine trends and main elements of Professional Money Laundering (PML) including laundering of Foreign Proceeds of Crime, the UAE-FIU selected sample of received STRs/SARs as well as international requests received from counterpart FIUs and has observed the following in the review:

A. Legal Entities (or Shell Companies) controlled by PMLs

The analysis conducted suggests that criminals – usually Organized Crime Groups - entrust PMLs to set-up mechanisms and infrastructures that will ensure the ill-gotten funds are untraceable. Hence, PMLs will transfer the funds to various LE accounts (with high possibility of being a front company or even a Shell Company) that are controlled by them, and then the funds might be moved or transferred through another layer of LEs and Shell Companies. This Money Laundering "ML" scheme might be in the same jurisdiction where the original crime has occurred, or from one jurisdiction to another, as part of a cross-border ML scheme.

B. Designated Non-Financial Businesses and Professions (DNFBPs) as PMLs conduit

DNFBPs, also known as "Gatekeepers", include lawyers, accountants, bankers, brokers, tax advisors, dealers in precious metals and stones, cryptocurrency exchange dealers, etc. This sector is capable of acting on behalf of its clients, exposed to vast amount of information and plays a critical role in overseeing the flow of funds. Criminals, especially Organized Crime Groups (OCGs) prefer DNFBPs due to their in-depth expertise on certain fields and their capability to conceal the origin of illicit funds. In PML perspective, DNFBPs are also termed as complicit actors or complicit professionals.

The analysis suggests that 'Gatekeepers' represent an essential element of PML. They can easily provide a well-structured ML mechanism - Starting by formation of Shell Companies (often in multiple jurisdictions), layering the funds and disguise its origin, engage in several investments, purchase assets specifically high-value items, as a typical pattern in the integration phase of money laundering, ending up with providing criminals with 'what seems to be' legitimized funds or assets.

On the other hand, DNFBPs are not always directly involved in the criminal activities. They could be unwittingly used by criminals. For this reason, this sector must be aware and abide by the obligations set within Federal Decree Law No. 20 of 2018 on Anti-Money

Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML Law") to prevent DNFBP's involvement in money laundering operations.

C. Recruiting Money Mules - Routing Fraudulent Foreign Proceeds of Crimes (Cybercrimes)

With the continuous advancement in modern technology, there are endless ways of acquiring money illegally, which ranges from basic theft or fraud to large-scale operations. In financial crimes, large-scale operations (such as cybercrimes) are mainly consisting of different networks in a number of jurisdictions globally to avoid detection and tracing of stolen funds. For that reason, cybercriminals tend to recruit 'Money Mules' to move illegally derived proceeds via either electronic transfers or physical cash movements.

As of the UAE-FIUs database pertaining to IRIs and ISDs, 14% of the intelligence reports received from counterpart FIUs found related to 'fraud'. Such reports constitute inquiries/information mainly on; Possible Fraud (46%), Possible Investment Fraud (13%), Possible Forgery (10%), Possible Fraudulent Wire Transfer (10%) and Possible Business Email Compromise Fraud (10%).

Based on the sample considered in this analysis it was found that, typically, the original fraudulent activity occurs in a foreign country, in which proceeds are routed to the UAE to accounts held by Individuals or Legal Entities, which could be either Fraudsters' allies or be unwitting Money Mules. The main concerns received were related to Cybercrimes (such as, scams, hacking, business email compromise, etc.) or related to other fraud types such as, forgery, and fraudulent tax evasion.

D. Recruiting Money Mules 'Cash couriers' for Cross-Border Cash Movements

Based on the analysis conducted by UAE-FIU during this project as well as a previous project on the "Abuse of Legal Entities", a common trend was noted involving individuals arriving to the UAE carrying large cash from various jurisdictions (predominantly high-risk). Cash transported is in different currencies and declared to the local customs authority in favor of a Legal Entity or an Exchange House.

In the first scenario, the LEs that couriers declared cash for is not the actual beneficiary of the funds. The LE is only being used as a front/shell company to receive funds on behalf of the exchange house. Whilst in the second scenario, the cash couriers straightforwardly declare that the funds are intended for the Exchange House.

Similar cases in the past indicated that this act is being done purposely by the exchange house for different reasons:

- The exchange house may be acting as an instrument to launder a third party's proceeds of crime and/or finance terrorism.
- The exchange house may not be willing to undergo the process of obtaining the "Letter of No Objection" from the CBUAE – Banking Supervision Department when importing and exporting banknotes from or to foreign institutions[3].

IV. Indicators and Guidance for Reporting Entities

The category of Professional Money-Laundering (PMLs) is the object of growing attention at national level and a mutual concern with relevant international organizations, given the threat they can represent to the integrity of financial and non-financial activities in general.

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, in particular foreign proceeds of crime. This topic required a strategic analysis in view of preventing and combating any ML/TF activity and supporting the adoption of adequate measures as well as guidance to Reporting Entities.

To some extent, PML indicators are similar to general ML/TF indicators, however, some elements found are more indicative of as a red flag of PML. The below list is not intended to be comprehensive and only provides examples of the most common ways by which a substantial risk can be detected.

On one hand, the presence of these indicators does not imply as such that the activity, or transaction, is suspicious. On the other hand, the apparent absence of these indicators does not exclude as such that the activity, or transaction, is suspicious. Reporting Entities shall carry out an overall weighting in the light of all available information, adopting the Risk-based approach, in assessing whether an activity, or transaction, is suspicious and whether there are conditions for filing an STR or SAR to the UAE-FIU.

[3] See CBUAE The Standards for the Regulations Regarding Licensing and Monitoring of Exchange Business ("the Standards") Version 1.10 dated February 2018, pp. 31-32: https://www.centralbank.ae/sites/default/files/2019-12/The%20Standards%20for%20Exchange%20Business%20in%20the%20UAE%20%28Version%201.10%29%20%E2%80%93%2001.03.2018%20for%20Issue%20%28Clean%29.pdf

In this context, the UAE-FIU has established the following possible indicators/red flags with relation to PML:

- An individual setting up multiple companies dealing in different lines of business simultaneously (one individual initially establishes the businesses; same address registered for most of the businesses; actual business activity not verifiable; each business is actually controlled by different individuals)

- Repeatedly depositing large cash amounts in the account which is supported by 'Cash Declaration forms' or also known as DRIC forms (Declaration regarding importation of Cash)

- Derogatory remarks or negative news found in external sources/public domain on the account holder or any of its counterparties, associates, signatories, UBOs, etc.

- Opening repository bank accounts under the name of a Legal Entity (to transmit funds from one jurisdiction to another swiftly; transfers justified as part of a normal business activity; used as pass-through accounts)

- Circulation of funds between several Entities accounts without any apparent reason, that might also suspected to be as 'shell companies' (no real business activity; incorporated for ML purposes exclusively)

- Setting up and using front companies (presence of real business activity; use to commingle legitimate and illegitimate funds, mainly used effectively in cash-intensive businesses)

- Transactions that involve 'Gatekeepers' which is found to be with no rationale or any apparent reason, specially to engage in several investments and purchase assets specifically high-value items

- Transactions with an Entity of a complex structure, in which the UBO is hard or cannot be identified (main purpose is to hide the UBO; to disguise funds transfers as capital transfer or normal business transaction)

- Funds received from offshore party(ies) subsequently routed to different personal or business accounts

- Providing fictitious documents to sustain the legitimacy of transaction (i.e. trade-based ML, seemingly "real" trade transactions supported by forged supporting documents, e.g. invoices, contract agreement, bill of lading, etc.),

- A group of customers uses similar contact information with unreasonable explanation (e.g. address, mobile number, e-mail address).

- The account holder suspected to be acting on behalf of a third party but not disclosing that information or is being controlled by someone else.

V. Example Cases

Case Example (1):

Summary: The UAE-FIU received an intelligence from a counterpart FIU regarding allegation made in relation to the involvement of a Free Zone Entity A (FZE A) in circumventing X sanction. In addition, UAE-FIU received multiple STRs raised against FZE A and other related counterparties. The reported subjects have conducted round circular pattern transactions through their own accounts and their counterparties. Wherein, they use the exact modus operandi and have multiple STRs filed against them. The subjects are operating high-risk business activities trading in oil and gas, wherein all their financial activities were mainly with FZ and offshore (shell) entities with no official business set-up. FZE A was dealing with high-risk suppliers fraught by allegations involved sanctions breaches and Money Laundering. It was further revealed that some of the counterparties had High-risk trade nexuses through public domain.

In addition, most of the counterparties' UBOs were from same nationality. Thus, it was suspected that the involved entities were conducting suspicious transactions through shell companies and trust companies in order to conceal the ultimate beneficiary owner, and circulate funds as part of layering phase of money laundering.

Consequently, the case was disseminated to the Law Enforcement Authorities and according to the feedback received, the case was further disseminated to State Security.

Case Example (2):

Summary: The UAE-FIU received multiple STRs from Bank A raised against two individuals; Subject A and Subject B (known to be A's friend). The reports were raised due to negative media reports, which stated that Subject A was a senior member of a criminal network in Country A. UAE-FIU received a request for information from Country A's FIU on the subjects; A and B, and the associated entities; i.e. Company A (registered in UAE) and Company B (Registered in foreign country).

The request revealed that Country A Authorities are conducting a parallel civil investigation to the criminal investigation for Money Laundering, allegedly being committed by Subject A. The taskforce's investigation purpose was to identify and trace ill-gotten assets with a view to restraining and forfeiting appropriate assets.

The analysis further revealed that Subject A is suspected to be involved in coordinating and facilitating money laundering activities from Country A to the UAE and other countries on behalf of the criminal network and other criminal networks. In addition, it was learnt that there were no known judicial proceedings in Country A. However, Country A's Criminal Intelligence are conducting the criminal investigation, whilst a civil investigation is being conducted by the Country A's Federal Police.

The UAE-FIU disseminated the case to Law Enforcement Authorities in the UAE for further investigation. The UAE-FIU had also sent multiple requests for information (ORFIs) to obtain further details on the international transactions involved in the case.

Case Example (3):

Summary: The UAE-FIU received multiple requests for information from counterpart FIU M regarding a major case involving a previous politically exposed person (Ex-PEP) who is the subject of criminal cases in his home Country M concerning corruption and Fraud. FIU M have identified list of linked natural persons, judicial persons and bank accounts in the UAE and requested the UAE-FIU's assistance in tracing and recovering the criminal funds by freezing the related accounts.

The analysis revealed that the said Ex-PEP used multiple individuals to set up a network of companies and bank accounts in various jurisdictions including the UAE, in order to launder proceeds of crime. Some of the professions noted of those said individuals (accomplices) was "Investor" or "Lawyer". it was further observed that mainly funds received in the UAE accounts were from offshore entities, which were subsequently transferred to personal accounts of the accomplices and further circulated among several (personal and Entities) related accounts. One of the main accomplices was found to be integrating high-value and luxury goods, and investing in multiple/unrelated lines of Business. Some financial transactions also indicated that the accomplice used Law firms to conceal the origin of funds and assets.

UAE-FIU have hosted physical and virtual meetings with FIU M and assured its full support and cooperation. The UAE-FIU have taken several actions some of which as follows:

- Search request to all financial institutions to identify bank accounts and provide relevant information including bank statements.
- Request to Ministry of Economy to identify real estates and companies.
- STR/SAR database search and analysis.
- Request to Advanced Passenger Information to identify exit and entry records and shipments.

Information and new links identified by UAE-FIU was shared with FIU M country to assist them with their analysis and investigation. Based on the analysis the UAE-FIU decided to freeze the bank accounts exercising its legal power to freeze for seven days through the Governor of the CBUAE. Freeze notice was sent to all financial institutions and an extension of freeze request was sent to public persecution, which was received and communicated to all financial institutions to freeze the natural person's account, their related companies' accounts and the account on which they are the authorized signatories. A report on the case along with a total frozen amounts was sent to public prosecution.

Glossary

Organized Crime Group

Is a category of transnational, national, or local groupings of highly centralized enterprises run by criminals to engage in illegal activity, most commonly for profit.

Professional Money Laundering

An individual, organization, or network (allegedly like these folks) that knowingly – rather than passively or unwittingly – provides third-party money laundering services to the direct earners of illicit proceeds in exchange for a commission, fee, or other type of profit.

Professional Money Launderer

Those individuals, organizations and networks that are involved in third-party money laundering for a fee or commission.

Professional Money Laundering Organization (PMLO)

Is when two or more individuals forming a structured group facilitating the laundering of illegal proceeds.

Professional Money Laundering Network (PMLN)

Usually operate in a larger scale and involve foreign jurisdictions, they may also include individual PMLs as well as PMLOs.