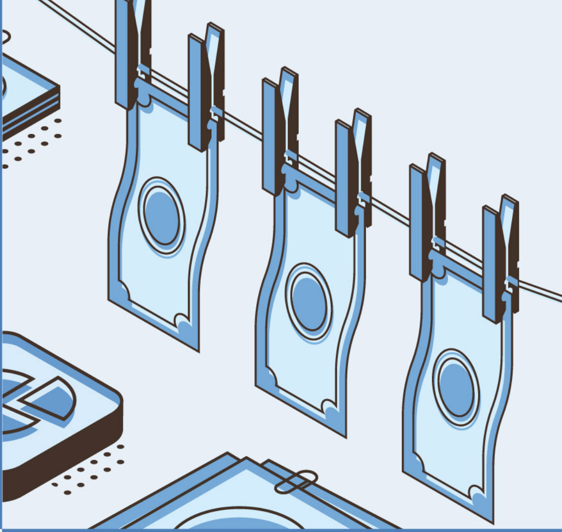
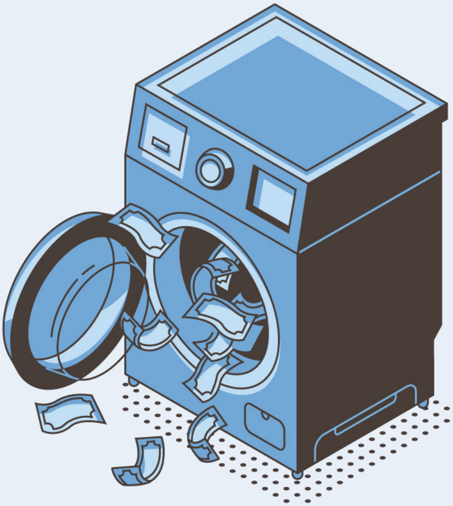
Money Laundering Typologies in the Republic of Moldova





Brochure for journalists

Controlling Corruption through Law Enforcement and Prevention (CLEP)

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

MONEY LAUNDERING TYPOLOGIES IN THE REPUBLIC OF MOLDOVA

Brochure for journalists

Controlling Corruption through Law Enforcement and Prevention (CLEP)

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

English edition
Published by the Council of Europe,
F-67075 Strasbourg Cedex
www.coe.int

Cover and layout design:
Foxtrot SRL, Chisinau
Printed by Foxtrot SRL, Chisinau
Circulation: 20 copies

This publication has been produced with the financial assistance of the European Union and the Council of Europe.

The views expressed herein can in no way be taken to reflect the official position of the European Union and/or Council of Europe.

For more information on the subject of the publication, please contact:
Economic Crime and Cooperation Division
Action against Crime Department
Directorate General
Human Rights and Rule of Law
Council of Europe
E-mail: contact.econcrime@coe.int
Internet: www.coe.int/corruption

CONTENTS

INTRODUCTION

This brochure provides a description of the *modus operandi* of criminal actors and money launderers that are relevant to risk context of the Republic of Moldova.

The National Risk Assessment (NRA) of the Republic of Moldova conducted in 2017 outlines major money laundering and terrorist financing (ML/TF) threats, vulnerabilities and risks the country is exposed to.

The main risk stems from predicate offences of drug trafficking, corruption, human trafficking, tax evasion and smuggling. Vulnerabilities for money laundering are the high use of cash, the opaque ultimate beneficial ownership structures and the use of shell companies for money laundering schemes. Corruption is recognised in the NRA as one of the most stringent problems in the Republic of Moldova.

Drug trafficking and human trafficking are the major money laundering threats coming from the crimes committed outside of country. Detailing the matter, the NRA indicates that the Republic of Moldova is not a country of drug production, but serves as transit point towards Eastern Europe and to a lesser extent it is a country of destination. On the human trafficking, one of the features is the systematic presence of the Organised Criminal Group (OCG) in the commission of crimes.

In terms of proceeds generating crimes committed domestically, corruption, tax evasion and smuggling are the main money laundering threats.

This brochure focuses on and describes typologies and *modus operandi* of criminals engaged in the following illegal activity:

- Cross-border professional money laundering schemes ('laundromat'-type);
- Drug trafficking (including non-contact sale of drugs via DarkWeb);
- Money laundering of corruption proceeds.

CROSS-BORDER PROFESSIONAL MONEY LAUNDERING (LAUNDROMAT-TYPE) SCHEMES AND MODUS OPERANDI

Although the famous 'Laundromat' scheme which was heavily reliant on use of the Republic of Moldova's financial system was a one-time affair, the risks related to trade-based money laundering (ML) schemes and use of offshore shell companies accounts remain relatively high.

Laundromat scheme was a traditional large-scale professional ML scheme arranged to move funds of third parties (including criminal actors). Professional money launderers (PML) are facilitators who provide money laundering services to criminals in exchange for a commission/fee. They are not involved in proceeds-generating criminal activity *per se* and can offer their services to a wide range of criminals (including those involved in drugs and human trafficking, fraud, cybercrime, corruption and embezzlement).

The Report on Professional Money Laundering issued by the Financial Action Task Force (FATF) in July 2018 provides a general description of PML business model and a wide range of mechanisms and instruments they use.

In general, financial schemes executed by PMLs consist of three stages[1]:

[1] FATF Report, July 2018, *Professional Money Laundering*, accessed in March 2020.

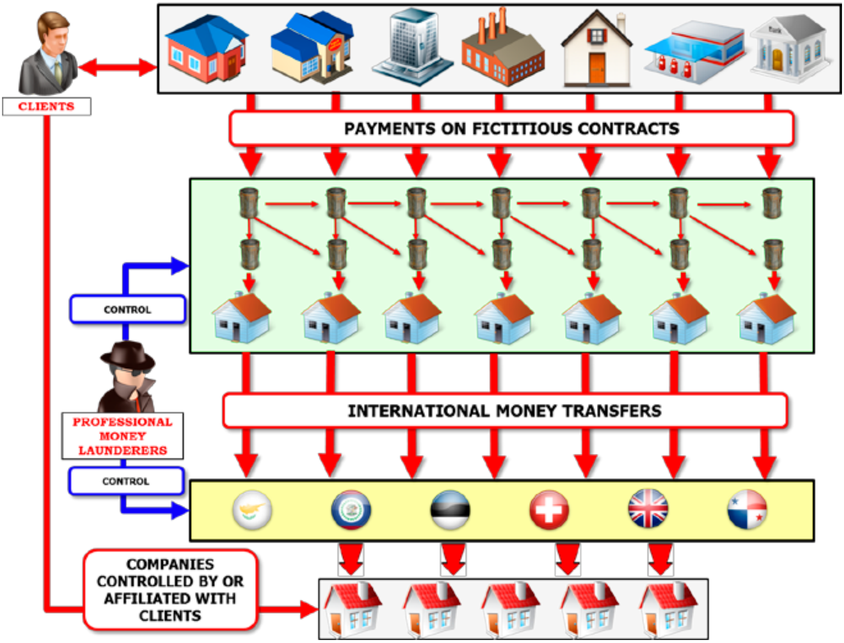

CLIENTS
PAYMENTS ON FICTITIOUS CONTRACTS
CONTROL
PROFESSIONAL MONEY LAUNDERERS
INTERNATIONAL MONEY TRANSFERS
CONTROL
COMPANIES CONTROLLED BY OR AFFILIATED WITH CLIENTS

Figure 1. Stages of ML scheme

STAGE I: CRIMINAL PROCEEDS ARE TRANSFERRED TO, OR COLLECTED BY, PMLS

In this first stage, funds are transferred, physically or electronically, to PMLs or to entities operating in their name. The manner of introduction of the funds into the money laundering scheme varies depending on the types of predicate offence(s)[2] and the form in which criminal proceeds were generated (e.g. cash, bank funds, virtual currency, etc.).

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 crypto-currency addresses, which can be accessed by the PMLs.

[2] An ML predicate offence is the underlying criminal activity which generated the laundered assets/property.

Examples:

- Cash is handed over to a cash collector who makes cash deposits on banks accounts.
- Criminal proceeds (for example, proceeds resulting from fraud, embezzlement and tax crimes) are allocated on bank accounts, afterwards these funds are transferred electronically to a first layer of companies that are controlled by the PMLs.

STAGE II: LAYERING STAGE EXECUTED BY INDIVIDUALS AND/OR NETWORKS

In the layering stage, the majority of PMLs use account settlement and complex mechanisms to make it more difficult to trace the funds. A combination of different money laundering techniques may be used as part of one scheme.

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.

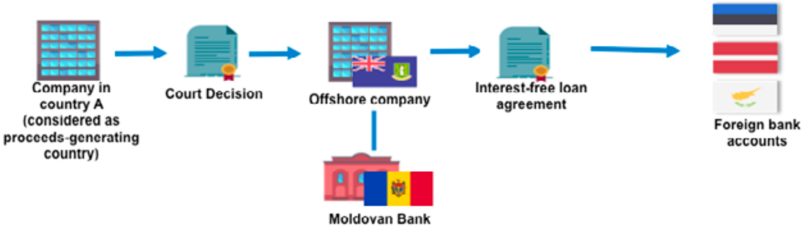

Company in country A (considered as proceeds-generating country)
Court Decision
Offshore company
Interest-free loan agreement
Foreign bank accounts
Moldovan Bank

Figure 2. Part of 'traditional' cross-border 3PML scheme that can be visible to Moldova. Proceeds of crime are transferred to the account of an offshore company opened with a Moldovan bank under fictitious court order, and almost immediately transferred to foreign bank accounts under loan agreement.

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).[3]

Similar *modus operandi* is used for **tax and customs duties evasion purposes**. Importing companies (for example, those located in the Republic of Moldova) transfer funds for 'imported goods' to a layer of intermediary shell companies to artificially increase their expenses and decrease the income tax to be paid. A portion of funds is then transferred to real exporters located abroad, and the rest of funds – moved further to accounts of offshore companies controlled by beneficiaries of this scheme.

USE OF MONEY MULES ACCOUNTS IN ML SCHEMES

A money mule is a person who receives money from a third party (or whose account is used by third party) and transfers it to another account or withdraws it in cash to hand it over. Money mules obtain a commission for these 'services'.

Criminals and, specifically, professional money launderers, widely use money mules accounts to move and launder proceeds of crime. Money mules can either conduct transactions themselves or just issue financial instruments (bank accounts, cards, e-wallets) on their names and provide them to third parties for payment.

Money mules accounts are widely used in DarkWeb – related schemes or in cybercrime (for example, phishing, malware attacks, online auction fraud and others).

Money mules are recruited in a number of ways, including:

[3] FATF Report, July 2018, *Professional Money Laundering*, accessed in March 2020.

- in a form of initially legitimate job offers related to 'money transfer services' sent via online job forums, social networks, emails, etc.;
- in a form of direct messages sent through messengers such as Viber, WhatsApp, Telegram;
- in person contacts (on the street).

Students and other people under 35 years old are the most targeted individuals who are offered to 'make easy money'. Money mules adverts usually state that they represent a foreign company recruiting 'national agents' to act on its behalf and to facilitate financial transfers. Sometimes these adverts emphasize that the transactions bear no risks, are '100% legitimate' and 'guaranteed'.

Even though money mules are not involved in the crimes that generate the criminal profits, they are accomplices as they facilitate the laundering of proceeds of crime.

Moldovan authorities detected cybercrime schemes based on money mules typology. For example, money mules accounts were mentioned in "Urgenta case"[4]. A group of individuals received funds on their Moldovan bank accounts from Romanian bank accounts. Funds were immediately withdrawn in cash through POS terminals (Point of Sales Terminals) at various bank branches in Chisinau. Further analysis revealed that Romanian bank accounts were credited from the UK bank accounts hold by Moldovan and Romanian nationals. Authorities identified that this financial scheme was used to move funds stolen with the use of Dridex and Dyrecare viruses.

Money mules accounts are widely used in financial schemes facilitating the DarkWeb illicit trade.

[4] Council of Europe, Moneyval, *Fifth round Mutual evaluation report of the Republic of Moldova*, 2019, page 57, accessed in March 2020.

LAUNDERING OF DRUG PROCEEDS. MODUS OPERANDI OF CRIMINAL GROUPS SELLING DRUGS VIA THE DARK WEB OR ONLINE MESSENGERS

With drug trade moving online, criminals change their modus operandi and employ the so-called non-contact sale of drugs that is supported with the use of new payment instruments, such as e-wallets and virtual assets. That should be a new but growing trend for the Republic of Moldova, substituting traditional sale of drugs with the use of cash.

The general *modus operandi* of criminal groups selling drugs via the Internet is the following.

- Customers of online drug stores when making their 'order' could choose between two means of payment – either transferring funds to indicated e-wallet (that belongs to online drug store) or to Bitcoin address.
- The financial scheme for the drug stores is usually arranged and managed by a financier and its network. The money laundering network is responsible only for moving funds and has no links to drug trafficking. Numerous e-wallets and debit cards are registered in the names of front men. This usually involves students who issue e-wallets and credit cards and sell them to members of money laundering network, being not aware of the criminal purpose of their further usage. Some e-wallets are used at the placement stage of the laundering process.
- Special software used by criminals allows to automatically change e-wallets that are used for drug payments and transfer funds to another level of mixing e-wallets when the limit is reached. Digital money is automatically moved through a complex chain of different e-wallets.

- Money from e-wallets is then transferred to bank cards and withdrawn in cash via ATMs (Automated Teller Machines). Withdrawals via ATMs are conducted by "cash coordinators" who have multiple debit cards at hand (all cards are usually issued on the names of straw men. After that, the cash is handed over to interested parties. In order to increase the complexity, proceeds can be re-deposited on a new set of debit cards and transferred to the organizers of drug trafficking criminal groups (usually located abroad).

Straw man is a person who provides its credit cards to criminals and knows nothing about their further use for criminal purposes.

- Funds from e-wallets can be also exchanged into Bitcoins via virtual currency exchangers. The Bitcoins are sometimes used to pay salaries to members of drug trafficking organisations, including low-level members such as small dealers and runners who facilitate the sale of drugs. The same financier can work with multiple owners of the Dark Web stores, distributing the laundered funds to the respective OCGs.

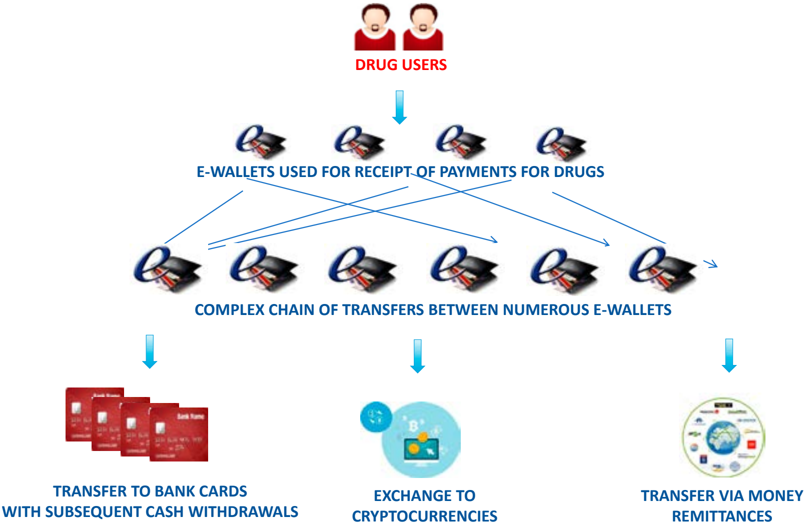

DRUG USERS
E-WALLETS USED FOR RECEIPT OF PAYMENTS FOR DRUGS
COMPLEX CHAIN OF TRANSFERS BETWEEN NUMEROUS E-WALLETS
TRANSFER TO BANK CARDS
WITH SUBSEQUENT CASH WITHDRAWALS
EXCHANGE TO
CRYPTOCURRENCIES
TRANSFER VIA MONEY
REMITTANCES

Figure 3. Movement of funds from DarkWeb illicit stores

LAUNDERING PROCEEDS OF CORRUPTION CRIMES

As acknowledged by the Moldova's National Risk Assessment (2017) and other international sources, corruption still remains widespread in the Republic of Moldova. Corrupted officials receiving bribes, in the majority of cases, rely on assistance of their close associates, including relatives, close friends, trusted partners and related legal persons and arrangements. These categories of individuals and their significant cash transactions, international money transfers and purchases of real estate and high-value goods require an increased focus.

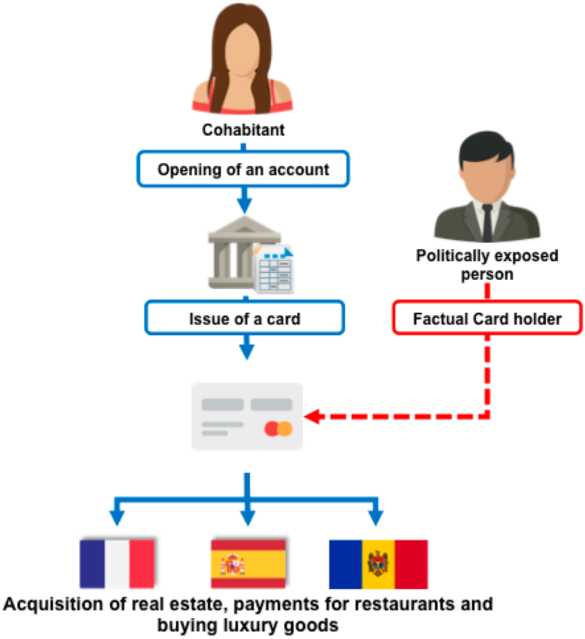

Cohabitant
Opening of an account
Politically exposed person
Issue of a card
Factual Card holder
Acquisition of real estate, payments for restaurants and buying luxury goods

Figure 4. Use of bank account belonging to an affiliated party by a PEP (Politically Exposed Person) to conceal transactions

Core elements in detection of financial flows stemming from corruption include:

- detection of unexplained wealth – assets and property of politically exposed persons (PEPs) and their relatives and associates which are not consistent with their declared income;
- detection of close associates to PEPs – their frequent contacts, relatives, friends, business partners, drivers and other individuals who can be used as third parties in financial transactions conducted on behalf of PEPs;
- detection of legal entities (including foreign companies) under control of PEPs and their close associates;
- detection of geographical centres of attraction (if a domestic PEP frequently travels to Spain or Italy, it is highly probable that he/she owns property or assets in this country).

Corruption is, in the vast majority of cases, interrelated with public funds, embezzlement and abuse of office, so, many conclusions can be made based on analysis of procurement data (including information on parties to contracts, their respective directors, members of tender board and other involved individuals, conditions of the contracts and their suspicious characteristics which reflect fluctuations of contract price, anomaly quick timelines of tender procedures, indication of very specific characteristics of goods and services, etc.)

The scheme below reflects a traditional 'kick-back' typology, where public funds provided to contractor are cashed out via shell companies and individuals' bank accounts, or moved abroad via accounts of offshore companies, and then handed over to PEPs, their close associates and owners of contractor engaged in embezzlement.

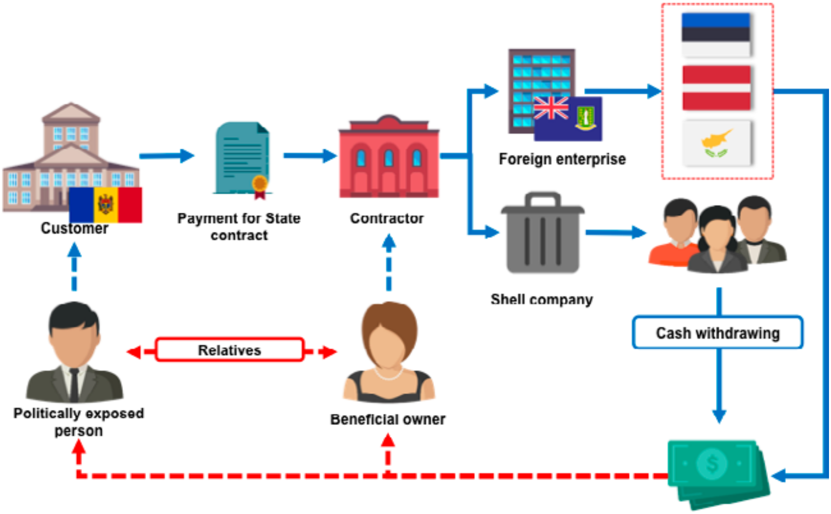


Figure 5. Typology of public funds embezzlement and corruption

CATEGORIES OF DATA AND INFORMATION RESOURCES THAT CAN SUPPORT JOURNALISTIC INVESTIGATIONS

The following categories of information are instrumental for detection and investigation of criminal and ML activity:

- **Commercial information** (including information on business activities of legal entities, staff numbers, financial accountancy that can be publicly available depending on country of incorporation and type of company – which is important both for assessing activities of real operating companies and for detection of shell companies which are used to move funds in ML schemes);
- **Contracts and tenders** (usually public and allows to obtain information on parties to contracts, their respective directors, members of tender board and other involved individuals, conditions of the contracts – including their suspicious characteristics which reflect fluctuations of contract price, anomaly quick timelines of tender procedures, indication of very specific characteristics of goods and services, etc.);
- **Ownership information** (including national open-source company registers, ownership data from various leaks and commercial databases – some of them allow to download all foreign companies owned or managed by nationals of a particular country with their personal details). This information is crucial for detection of beneficial owners, affiliated networks, conflicts of interest checks, corruption risks detection;
- **Customs information** (including open-source basic information on involvement of legal entities in trade activities);
- **Public income information** (especially important for the purposes of detection of corruption and public funds embezzlement schemes

via detection of discrepancies between declared income of PEPs and their relatives and factually owned assets and property – and further investigation into an unexplained wealth);

- **Technical and geo-location information** (including IP addresses, for example, in block-chain transactions);
- **Communication information** (including mobile phone numbers, accounts names);
- **Social relationship** (including information from social networks on 'friends' and contacts);
- **Criminal information** (including publicly available national police databases, Interpol lists, various 'dirty laundry websites' etc.);
- **Commercial courts data** (including for the purposes of detection of falsified court orders which were used as a pretext for cross-border money transfer in Laundromat schemes);
- **Various open-source lists and registries**, including domestic and foreign public PEPs lists, data leaks.

LIST OF ONLINE RESOURCES (PUBLICLY AVAILABLE DATABASES) TO SUPPORT MONEY LAUNDERING INVESTIGATIONS

1. **Offshore Leaks Database:**

▬ *https://offshoreleaks.icij.org*

▬ The database is maintained by the International Consortium of Investigative Journalists. It contains information on more than 785 thousand offshore companies, foundations and trusts from the Panama Papers, the Offshore Leaks, the Bahamas Leaks and the Paradise Papers investigations.

2. **The Investigative Dashboard Catalogue of Research Databases:**

▬ *https://investigativedashboard.org/databases*

▬ The database contains web-links to numerous company registries, land and real estate registries, court orders databases, patent office information and other publicly available information all over the world (grouped by countries and regions).

3. **OCCRP Aleph Database:**

▬ *https://aleph.occrp.org*

▬ The database is a global archive of research material for investigative reporting containing various leaks, sanctions and PEPs lists, property and companies databases, contracts, procurement information, etc.

4. **Marine Traffic Live Map:**

- *www.marinetraffic.com*
- Global Ship Tracking Intelligence map showing the current position and basic information about marine vessels.

5. **IP Geo-location Finder:**

- *https://www.iplocation.net*
- The database provides support in identifying approximate location of an IP user (IP address).

6. **Free search of Politically Exposed Persons:**

- *https://namescan.io/FreePEPCheck.aspx*
- The database provides a scan for PEPs and their Relatives and Close Associates.

7. **Interpol Wanted Persons search:**

- *https://www.interpol.int/en/How-we-work/Notices/View-Red-Notices*
- Contains public Red notices for wanted persons (Red Notices are issued for fugitives wanted either for prosecution or to serve a sentence. A Red Notice is a request to law enforcement worldwide to locate and provisionally arrest a person pending extradition, surrender, or similar legal action).

USEFUL BIBLIOGRAPHY TO SUPPORT ML INVESTIGATIONS

1. Egmont Group Bulletin, July 2019, *Professional Money Laundering Facilitators*;
2. Egmont Group Bulletin, July 2019, *Business Email Compromise Fraud*;
3. Egmont Group Bulletin, July 2019, *Counter Terrorist Financing Project – Lone Actors and Small Cells (Public Summary)*;
4. Egmont Group, Public Summary, July 2019, *FIU Tools and Practices for Investigating Laundering of the Proceeds of Corruption (Public Summary)*;
5. FATF – Egmont Group, 2018, *Concealment of Beneficial Ownership*;
6. FATF Report, July 2018, *Financial Flows from Human Trafficking*;
7. FATF Report, July 2018, *Professional Money Laundering*;
8. FATF Report, January 2018, *Financing of Recruitment for Terrorist Purposes*;
9. FATF Report, October 2015, *Money Laundering Through the Physical Transportation of Cash*;
10. FATF, October 2015, *Emerging Terrorist Financing Risks*;
11. FATF Report, July 2015, *Money laundering and terrorist financing risks and vulnerabilities associated with gold*;
12. FATF Report, June 2014, *Financial flows linked to the production and trafficking of Afghan opiates*;
13. FATF Report, June 2014, *Risk of terrorist abuse in non-profit organizations*;
14. FATF Report, October 2013, *The role of Hawala and other similar service providers in money laundering and terrorist financing*;
15. FATF Report, June 2013, *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*.

Notes

Notes

Notes

This brochure provides a description of the money laundering (ML) typologies relevant to the risk context of the Republic of Moldova. It also describes the methods used by criminals in regard to specific ML offences and analyses concrete examples and schemes aimed to support the readers understanding of most common steps used during the money laundering process. The brochure also aims at providing journalists with information and resources that can support ML investigations as well as a list of online publicly available database useful for this purpose.

www.coe.int/clep

ENG