



**APPROVED BY THE DECISION OF THE GOVERNOR
OF THE CENTRAL BANK OF ARMENIA NO 1/185A
FROM 06.06.2025**

T TYPOLOGY 15
MONEY LAUNDERING FACILITATED THROUGH THE USE OF THIRD-PARTY
INTERMEDIARIES

YEREVAN 2025

CONTENT

Chapter 1. Scope of application	3
Chapter 2. Introduction	3
Chapter 3. Fraud types	3
Chapter 4. Scheme description	6
Chapter 5. Criteria description	7
Chapter 6. Conclusion.....	7

Chapter 1. Scope of application

The money laundering scheme outlined in this typology may involve certain reporting entities as defined under the RA Law “On Combating Money Laundering and Terrorism Financing,” specifically:

- a. banks;
- b. entities engaged in money (currency) transfer services;
- c. organizers of online games of chance and lotteries.

One of the aims of this analysis is to raise awareness among the public and law enforcement agencies about the different fraud and money laundering schemes connected to it.

Chapter 2. Introduction

This analysis was carried out in light of the noticeable increase in recent years in the number of alerts received concerning various types of fraud, including the laundering of criminal proceeds generated through such schemes.

The typology is intended as a guiding (advisory) resource and has been developed based on publicly available international publications on prevailing trends, as well as trends observed and analysed within the Republic of Armenia. In part, this analysis builds upon earlier reports—namely, “*On the Nature, Types, and Characteristics of Fraud Schemes Using the Mass Marketing Model*” and “*On Fraud Schemes Involving Business Offers with Externally Attractive Conditions*”—and expands on the findings presented in those publications.

Within this typology, the term “fraud” is used in a broad sense. The scenarios (examples) described may involve elements of several criminal offenses as defined by the Criminal Code of the Republic of Armenia, such as fraud (Article 255), computer theft (Article 257), and others. For the purposes of this typology, fraud refers generally to unlawful acts aimed at misappropriating funds or other assets from individuals or legal entities through deception or abuse of trust.

Given the diverse nature of criminal behaviour, identifying fraud and the schemes used to launder the resulting proceeds requires familiarity with the tools and methods employed, as well as the warning signs that may indicate their use. Accordingly, the sections that follow provide:

- An overview of fraud types;
- A description of possible money laundering schemes involving proceeds of fraud;
- A breakdown of criteria pointing to the laundering of fraud-related funds.

Chapter 3. Fraud types

Fraud schemes employ a wide range of methods and techniques, but for the purposes of this analysis, it is suggested to categorize and differentiate them based on the type of false information presented to the victim and the specific tactics used. Accordingly, the following types can be identified:

Fraud involving consumer goods and services

In this scheme, the perpetrator creates a website or sets up an account on a popular online marketplace or social media platform to advertise goods or services they have no intention of delivering (in some cases, the goods may be fake or worthless). These offers typically include appealing conditions—such as prices noticeably lower than market rates. Items or services with high consumer demand, like household appliances, electronics, or loan services, are commonly chosen. The victim is tricked into making an upfront payment, which is then stolen without the promised product being delivered or the service provided. This method is also commonly used for committing fraud involving the theft of personal data. For example, the victim may be redirected to a website under the pretence of making a purchase, where they are prompted to enter their bank card information. The perpetrator then uses this data to steal funds from the victim's account.

Employment fraud

In this scheme, the perpetrator posts a job advertisement online containing false or misleading claims, often featuring overly attractive conditions—such as unrealistically high salaries for remote work or highly flexible schedules. Before the victim can begin the supposed job, they are typically asked to:

- Pay a fee, allegedly for administrative purposes such as paperwork or other fictitious organizational steps, which is then stolen;
- Complete an application or questionnaire requesting personal information, including banking details, which the perpetrator uses to gain access to the victim's bank account and steal funds or take out loans in the victim's name. This personal data may also be exploited to commit other crimes using the victim as an unwitting intermediary.

Investment fraud

In this scheme, the perpetrator deceives the victim with false promises of high returns, encouraging them to invest in non-existent financial instruments—often linked to emerging technologies such as crypto-assets. Typically, a website or app is created to display the victim's investments and alleged earnings. These figures are entirely fictitious and can be manipulated by the organizer at any time to create the illusion of profit.

In some instances, the perpetrator allows the victim to withdraw a small portion of their investment—usually from the initial funds deposited—in order to build trust in the scheme.

Once the organizer has stolen the bulk of the victim's funds, they may continue to exploit the victim under various pretences to extract additional money. For example, the organizer might impersonate:

- A law enforcement official, claiming they can help recover the stolen funds in exchange for a fee;
- A tax authority representative, demanding payment of alleged taxes on the investment, supposedly required for withdrawal;
- A bank employee, requesting a commission for identification or another fictitious process, supposedly necessary to transfer the accumulated funds through the banking system.

Fraud committed in the name of a trusted person

In this scheme, the perpetrator contacts the victim while posing as someone the victim trusts — either an individual or an organization — due to personal relationships or other circumstances. A key feature of this type of fraud is the deliberate creation of a false belief in the victim, often aimed at provoking fear, urgency, or anxiety. Using tools such as email, social media, messaging apps, or even artificial intelligence, the perpetrator may impersonate:

- An employee of a government agency (e.g., tax authority, law enforcement) and demand payment under the threat of legal action or other negative consequences;
- A representative of a private organization (e.g., a reputable bank, IT company, or charity), requesting money or bank account details under a false pretext—such as preventing fraud or a cyberattack, settling a fabricated debt, claiming lottery winnings, making a donation, or similar scenarios;
- A family member or friend (often using personal information obtained from social media), who urgently asks for money under a fabricated story—for example, to cover hospital bills. Frequently, victims are chosen based on having a family member or friend who lives abroad. The fraudster uses this detail to justify the need for help—claiming, for instance, that payment must be made using financial tools only available in the victim’s country—or to explain why immediate repayment is impossible, citing reasons like time zone differences or banking hours that prevent money transfers.

Romance-based fraud

In this type of fraud, the perpetrator builds a romantic relationship with the victim, gradually gaining their trust and convincing them of the relationship’s authenticity.

These schemes often target individuals who may be emotionally vulnerable for various reasons. The perpetrator typically creates a fake identity on social media or dating platforms—using photos of attractive individuals, fabricating details about wealth, social status, or occupation—to present an appealing and credible persona.

Once a romantic connection is established, the fraudster begins requesting money under various false pretences, such as emergency travel needs or medical expenses. These requests often involve transferring funds abroad. In some cases, the fraud escalates to blackmail. The perpetrator may threaten to publicly share nude or semi-nude images of the victim—images that were either voluntarily sent or fabricated using artificial intelligence or other digital tools.

The trust developed through the romantic relationship can also be exploited to carry out other forms of fraud, such as investment scams, where the perpetrator, posing as a trusted partner, encourages the victim to invest in fake financial instruments.

Fraud through abuse of organization’s internal networks

In this scheme, the perpetrator gains access to an organization’s internal systems with the intent to deceive its employees, partners, or other affiliated individuals.

Specifically, the fraudster may infiltrate the organization’s email or other communication platforms and use the compromised data to send messages that appear to come from legitimate sources within the organization. These messages may be sent from actual accounts

or from spoofed email addresses that closely resemble official ones (often differing by just a single character).

Using this access, the perpetrator may instruct employees to carry out unauthorized fund transfers or send fake invoices to the organization's partners, exploiting the trust and routine workflows of the organization for financial gain.

Fraud using stolen or falsified personal information

In this scheme, the perpetrator uses stolen or fabricated personal data to obtain money or other benefits. This information may include, for example, a person's full name, date of birth, bank card details, login credentials for online accounts, biometric data (such as fingerprints collected from electronic devices), and more.

Acting under another person's identity, the perpetrator can use this data to purchase goods or services, apply for loans, withdraw funds from the victim's bank account, or use the account to launder illicit proceeds.

To obtain personal information, the fraudster may employ various techniques—such as malicious software, phishing attacks, the illegal trade of personal data, creation of fake websites that closely mimic legitimate ones, misleading advertisements, or deceptive emails, text messages, or phone calls.

The seven types of fraud described above are not exhaustive; fraud can take many other forms. Moreover, certain schemes may involve elements from multiple categories at once, making them more complex and harder to detect.

Chapter 4. Scheme description

The observed trends suggest that fraud involving relatively large sums of money is often carried out by organized criminal groups—structured and stable entities formed specifically to commit various types of crime. These groups frequently operate across borders, with members based in different countries, each playing a defined role within the fraud scheme.

For instance, the leader of such a group may set up a call center in a country other than their own place of residence or main area of interest. The purpose of the call center is to reach out to individuals in other countries, establish trust or mislead them, and ultimately steal their assets—commonly by convincing them to make false “investments.”

Prior to executing the fraud and obtaining criminal proceeds, the organizer typically prepares in advance to move the funds quickly in order to launder them. To enable this rapid movement, they often rely on financial services that allow instant transactions, such as card payments.

In the early stages of laundering, the stolen funds are typically funnelled through:

- **Indirect intermediaries**¹ – individuals who receive money from unknown sources and then, at the direction of a third party, transfer those funds to others;
- **Fictitious companies** – businesses that, despite being legally registered, have no actual presence, assets, operations, or other characteristics of genuine activity.

¹ See details in “Money laundering facilitated through the use of third-party intermediaries” typology.

Transfers designed to conceal the source of funds are often sent to personal bank accounts or digital wallets of individuals trading crypto assets through Crypto Asset Service Providers (CASPs) operating in poorly regulated or unregulated jurisdictions, or via so-called peer-to-peer (P2P) methods. In some cases, illicit funds are also funnelled into gambling companies to top up individuals' gambling accounts.

Recent trends show that crypto-assets are increasingly being acquired—either directly or indirectly—through criminal activities. After circulating through various crypto accounts, these assets are then converted and integrated back into the financial system via CASPs, appearing as legitimate proceeds from the sale of crypto-assets.

Chapter 5. Criteria description

The following are some criteria that may suggest an attempt to launder funds obtained through fraud:

- Immediately after the account is opened, instant transactions—often card-based—are carried out that do not align with the stated purpose of the account.
- The account regularly receives incoming funds, followed by immediate cash withdrawals or transfers intended to rapidly bring the balance back to zero.
- The client regularly carries out transactions that do not align with their business profile—for instance, cash withdrawals from foreign ATMs using a card, or incoming international transfers from various individuals.
- A significant portion of the funds received from different individuals or deposited in cash into the client's account is used to purchase virtual assets (e.g., payments made on foreign CASP websites).
- The client, a newly established legal entity, engages in frequent, high-volume transactions, including cross-border ones, without any clear economic or legitimate purpose.
- The legal entity conducts transactions with organizations whose business activities differ significantly from its own.
- The client either has no knowledge of the source of funds transferred to their account or the purpose of the transactions, or claims to be conducting transactions on behalf of another person.
- The legal entity's name is frequently changed to incorporate well-known foreign terms or phrases, with no clear reasoning or logic behind the changes.
- There are requests to reverse funds, often citing alleged fraud.
- The client or their counterpart operates online platforms that exhibit characteristics consistent with fraudulent schemes—for example, offering investment services without holding the necessary licenses or permits.

Chapter 6. Conclusion

Schemes carried out using the methods and tools outlined in this typology may aim to conceal or misrepresent the origin, movement, and beneficial ownership of funds. To determine whether schemes involving the laundering of funds obtained through fraud are present, the

reporting entities identified in Chapter 1 of this typology should adopt a comprehensive approach. This includes placing emphasis on and combining both the data collected during the establishment of the business relationship—specifically regarding customer identification and business profile—and the findings from ongoing monitoring of the customer or their transactions.

In this context, it is essential to give particular attention to the criteria outlined in Chapter 4, as they are considered key to identifying the schemes in question. As a preventive measure, reporting entities are expected to conduct adequate awareness-raising efforts concerning situations that meet these criteria, aiming to protect customers from becoming victims of potential fraud.

It is important to note that the situations and criteria described in this typology are not exhaustive and should not be interpreted rigidly, as criminals continuously adapt their methods in response to evolving socio-economic conditions, new systems, and rapid technological developments. Therefore, in practice, fraudulent schemes may arise that only partially align with the typology's criteria or fall entirely outside of them.