



CENTRAL BANK OF THE
REPUBLIC OF ARMENIA

FINANCIAL MONITORING CENTER

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

TYPOLGY 16
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. Scheme description	3
Chapter 4. Criteria description	4
Chapter 5. Conclusion	5

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.

Chapter 2. Introduction

In recent years, there has been a relative increase in the number of reports concerning various predicate offenses, including money laundering, committed through accounts opened at the direction of third parties.

To characterize and detect criminal schemes involving third-party direction, it is essential to understand the methods and mechanisms employed in their execution, as well as to identify indicators or red flags related to the client’s business profile or transaction activity, the presence of which may suggest the possible occurrence of a money laundering scheme.

Chapter 3. Scheme description

Operations carried out under the direction of third parties are instrumental in the preparation and execution of various criminal offenses. These operations are facilitated by so-called “indirect intermediaries”¹, who assist in the movement of proceeds of crime by obscuring the origin, destination, and ultimate beneficiaries of the funds, as well as concealing the true organizers of the criminal activity.

In essence, “indirect intermediaries,” are individuals who receive funds from unidentified sources and, under the instruction of a third party, subsequently transfer the funds to other individuals². Such operations may be conducted through a bank account/card, a payment account (electronic wallet), a gaming account, or a cryptoasset account (hereinafter referred to as an account), and may also involve granting third parties online access to remote account management (e.g., username and password). Furthermore, these funds may circulate in both cash and non-cash form.

“Indirect intermediaries” are part of a criminal scheme, though in some cases they may be unaware of their involvement in illicit activity. In this context, “indirect intermediaries” are conventionally classified as follows:

- *Uninformed “indirect intermediaries”*, who are unaware that they are participating in a criminal scheme. These individuals are often recruited by criminals through fake job offers or online dating platforms and are asked to use their personal accounts to receive or transfer funds. In some cases, the accounts are accessed or operated without the knowledge of the actual account holders.
- *Informed “indirect intermediaries”*, who disregard clear red flags and knowingly “turn a blind eye” to suspicious transactions conducted through their accounts. For example, such

¹ “Дроппер” (“dropper”), “money mule”, and other similar foreign terms are often used.

² There are also cases where individuals have spread advertisements offering to sell their bank account information in order to receive commissions.

individuals may be notified by a financial institution about suspicious activity, yet continue to facilitate the transactions.

- *Participating “indirect intermediaries”*, who are fully aware of their role in the illicit scheme and actively contribute to its execution. These individuals may open multiple accounts at different financial institutions, promote their services, and in some cases, also recruit other “indirect intermediaries.”

Criminals typically recruit “indirect intermediaries” by offering commissions—usually in the form of a lump sum, a percentage of the circulated funds, other material benefits, or promises thereof. While recruitment methods vary, they most commonly involve online job offers. The assigned “work” almost always consists of depositing or withdrawing funds (including in cash), as well as providing remote access credentials for account management. Typically, criminals:

- Entice targets with offers of high salaries, get-rich-quick schemes, high-yield investment opportunities, or other unrealistic and fictitious promises (e.g., claims that no experience or education is required, or that the work can be done entirely remotely without physical presence).
- Target socially vulnerable, financially inexperienced, unemployed or low-income individuals—often young people, students, or pensioners.
- Provide guidance on how to respond to inquiries or documentation requests from financial institutions to avoid the reporting of suspicious transactions or the application of enhanced due diligence measures.

Chapter 4. Criteria description

The operations of indirect intermediaries can, in practice, be used in schemes aimed at laundering proceeds derived from various predicate offences. Among the most frequently encountered underlying crimes are internet fraud, cyber-enabled theft, online extortion, Ponzi or pyramid schemes, and illicit drug trafficking³. The possible money laundering schemes described are typically characterized by at least one of the following indicators:

- The client is unable to provide reasonable, substantive explanations:
 - for the discrepancy between the declared income (salary) or expected turnover volumes at account opening and the actual account activity;
 - for numerous incoming and outgoing transactions conducted through newly opened or previously “inactive” accounts.
- Within a relatively short timeframe, the account receives numerous deposits followed by subsequent transfers—sometimes occurring just one minute apart—to various parties, including local or foreign individuals providing crypto-asset-related services.
- Payments for essential living expenses (such as utilities, food, or other consumer goods) are notably absent from transactions conducted through the account.
- The client reports that: a) they are conducting transactions under the instructions of a third party; b) they have granted full online access for remote account management to a third party; or c) they are completely unaware of the transactions being carried out on their account.

³ In practice, a reporting entity may identify its client as an indirect intermediary, for example, upon receiving a negative alert from a partner institution or a member of the public indicating that funds credited to the client’s account (including relatively small amounts ranging from AMD 10,000 to AMD 100,000) originated from fraud or another online crime.

- The account is used to make numerous small-value transfers⁴ to various individuals as commission payments; the senders are often informed or complicit indirect intermediaries who, in turn, recruit others.
- The customer is unemployed (for example, a student) yet conducts numerous transfers and receipts.
- Multiple customers access accounts from the same remote online system or device (such as a phone) or provide identical contact details (such as an address or phone number) during account opening, without a reasonable explanation.
- The customer uses a virtual address or phone number during the identification process to conceal their actual physical location.

Chapter 5. Conclusion

Schemes using the methods and tools described in this typology may aim to conceal or misrepresent the source of funds, their movement, and the beneficial owners.

To identify potential criminal schemes executed under the direction of third parties, reporting entities outlined in Chapter 1 of the typology should adopt a comprehensive approach — integrating information gathered during customer identification and profiling at account opening, along with insights gained from ongoing monitoring of the customer and their transactions. Within this context, it is essential to pay close attention to the characteristic criteria outlined in Chapter 4, which are considered key for detecting the schemes described.

However, the situations and criteria presented in the typology are neither complete nor exhaustive and should not be interpreted rigidly, as criminals continuously adapt to evolving socio-economic conditions, systems, and rapidly advancing technologies. Therefore, in practice, other manifestations of crimes committed under the direction of third parties may occur that only partially align with, or fall outside of, the criteria detailed in this typology.

⁴ For example, between AMD 1,000 and AMD 5,000.