



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 17
**LAUNDERING THE PROCEEDS OF DRUG TRAFFICKING THROUGH THE USE OF
CRYPTOASSETS**

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.....	6

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

With the advancement of modern technologies, information and telecommunication systems have become widely utilized in drug trafficking in recent years. These systems enable the operation of drug trafficking networks in the digital space, offering anonymity, speed, and continuity in illicit transactions. As a result, trafficking groups can rapidly gain visibility among potential buyers, while tracing the financial flows derived from drug sales becomes significantly more challenging.

Alongside the growing use of telecommunications applications for drug distribution, there has been a marked increase in the use of cryptoassets for receiving payments. In many cases, the proceeds from drug sales are subsequently disguised and presented as profits from the buying and selling of cryptoassets. This trend is largely driven by technological characteristics inherent to cryptoassets, including user anonymity, global accessibility, the absence of central issuers in some cases, the irreversible nature of transactions, and the often limited application of recordkeeping and transparency standards.

Chapter 3. Scheme description

Drug trafficking groups establish online storefronts within various telecommunication platforms to promote and facilitate the sale of different types of narcotics. Within these organized networks, members typically assume distinct operational roles, including sourcing, packaging, distributing drugs, concealing them in pre-determined locations, photographing the hiding spots, and sending precise geolocation details to customers.

For example, a group leader may compensate a member responsible for placing drugs in a hiding spot by transferring a payment—ranging from USD 3 to 10—via electronic wallets, bank cards, or cryptoasset accounts. To receive payment for the drugs sold, these groups provide buyers with designated cryptoasset wallet addresses and instruct them to engage in online correspondence with cryptoasset service providers (CASPs) to facilitate the transfer of funds.

Once contact is established with the CASP, buyers transfer the drug payment—either in cash or via non-cash deposits—to the CASP’s electronic wallet or bank account to purchase a cryptoasset. The CASP, in turn, transfers the acquired cryptoasset from its own wallet to a wallet controlled by the drug trafficking group, as specified by the buyer.

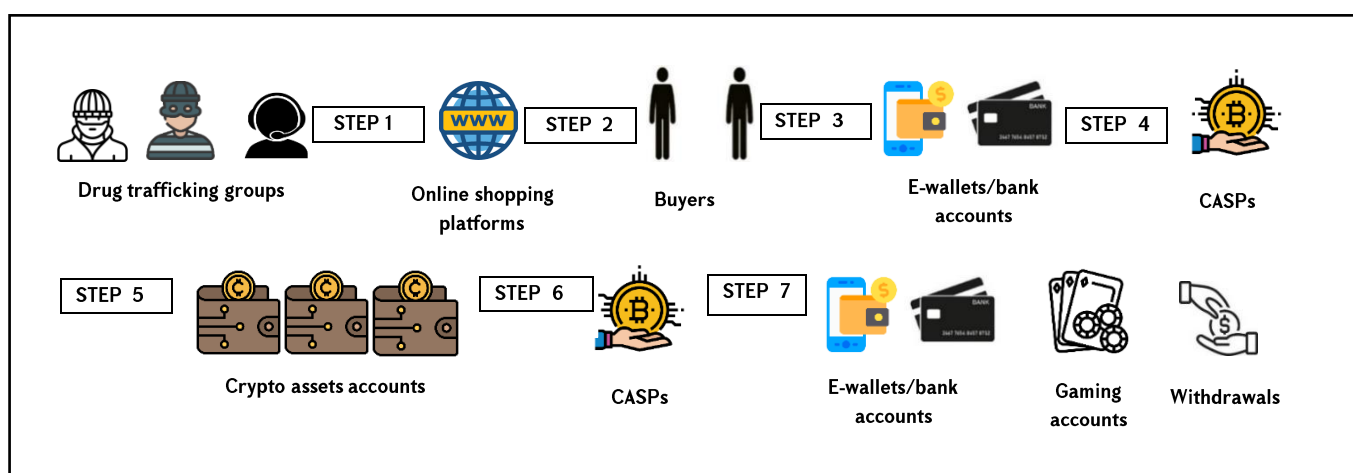
As part of this payment infrastructure, trafficking groups often use multiple “unhosted” or “self-custody” wallets to collect initial payments. These wallets are typically used to receive

one or a small number of payments, a tactic that reflects classic layering methods aimed at reducing traceability and complicating transaction monitoring.

Subsequently, drug trafficking groups engage in the following activities to further the laundering of proceeds derived from drug sales:

- Cryptoassets obtained from drug trafficking are funnelled—often through a series of chain transactions—into central wallets controlled by key group members, and are often transferred disguised as “salaries”¹.
- The consolidated cryptoassets are then converted into Armenian drams or other fiat currencies via local or foreign cryptoasset service providers (CASPs).
- These operations, including the liquidation of cryptoassets into fiat currency, are frequently conducted through electronic wallets, bank cards (accounts), or cryptoasset accounts that are registered under third-party names² but are effectively controlled by members of the trafficking network.
- The resulting funds — whether held in the personal wallets, bank cards, or accounts of group members, or in third-party accounts under their control — are used in both cash and non-cash forms for a range of purposes. These include purchasing property, covering personal expenses, topping up online gambling accounts, and other forms of asset integration.

The diagram below illustrates the scheme used to launder proceeds from drug sales



Chapter 4. Criteria description

To identify potential money laundering linked to the illicit sale of drugs, reporting entities should monitor for certain red flags or indicators that are considered critical for detecting the scheme described in this typology. These include:

¹ For example, to plant drugs in a hiding place.

² Other individuals may include family members, friends, as well as “indirect intermediaries” as described in the “Third-Party Money Laundering” typology.

- The presence of numerous electronic wallets and bank accounts opened under the names of the same individuals and/or their family members, where no clear economic or legitimate purpose can be established.
- The customer conducts the majority of their financial transactions during night-time hours.
- A high volume of incoming transfers to the customer's electronic wallets or bank accounts, typically in the range of AMD 15,000 to 100,000.
- The funds credited to these wallets and accounts largely originate from the sale of cryptoassets, while transactions related to the purchase of cryptoassets are either absent or minimal in number.
- The client has no idea about the purpose of the transaction and the source of the funds involved in the transaction, or does not recall, evades, or provides inconsistent information about the types of cryptoassets sold by them.
- The client uses crypto "mixers"³, "tumblers"⁴, and/or receives funds from the sale of cryptoassets of the "privacy coins"⁵ type.
- The client receives frequent small-value transactions in irregular, non-rounded amounts (e.g., AMD 1,975; AMD 3,160; AMD 3,950)⁶,
- There is a short time interval between receiving bank transfers and conducting cash withdrawals, or the customer performs substantial cash withdrawals from multiple bank accounts within the same day
- Payments for other people's vital needs are regularly made from the customer's electronic wallet or bank account (for example, payments for utilities, communication services, payments for parking, food, or other goods).
- A customer who has shown little or no prior financial activity suddenly becomes active, or the volume and frequency of financial transactions are inconsistent with the customer's known economic profile or declared business operations.
- The client reports that they are making transactions on the instructions of a third party or have fully provided online access to the account/wallet for remote management by a third party.
- The logic and movement of the client's transactions indicate that the transactions are made by a third party (for example, the client permanently resides in the "X" location, but the transactions are made from ATMs or POS terminals located in the "Y" location).

3 "Mixers" are service providers that split their clients' cryptoassets and conduct bulk transactions between their own cryptoasset accounts in order to obscure the traceability of transactions (e.g. CoinJoin, Wasabi Wallet, Samurai Wallet).

4 "Tumblers" are service providers that fragment their clients' cryptoassets and perform multi-layered transfers between newly created and reserve cryptoasset accounts they manage in order to obscure the traceability of transactions (e.g. Tornado Cash, Join Market).

5 Cryptoassets of the "privacy coins" type allow individuals to remain anonymous or make anonymous private transfers (e.g. Monero, Dashcoin, Zcash, Grin, etc.).

6 These funds are mainly transferred to group members after placing the drugs in hiding places; see the "Scheme Description" chapter for details.

- The client regularly uses cryptoasset trading platforms⁷, through which they register and use multiple “unhosted” or “self-custody” cryptoasset accounts.
- The same customers regularly place bets on games with a low probability of losing.
- The customer regularly participates in online gambling with the same people, during which they lose all their money to the same people by the method of “deliberate losses”, or these people lose to them (for example, poker, tournaments, roulette⁸).
- The customer regularly replenishes their gaming account with a large amount of money, but only bets with a portion of these funds, and after a short time—regardless of the outcome—the remaining funds are withdrawn.

Chapter 5. Conclusion

The schemes and steps presented in this typology may serve the purpose of concealing or disguising the origin, true nature, movement, and beneficiaries of the proceeds of drug trafficking, and of giving those criminal proceeds a legitimate appearance.

At the same time, the situations, characteristics, or criteria described in the typology are not comprehensive or exhaustive and should not be interpreted rigidly, as criminals continuously adapt and employ new methods in response to evolving socio-economic conditions, systems, and rapidly advancing technologies. Accordingly, in practice, instances of laundering drug trafficking proceeds may arise that only partially align with the characteristics or criteria outlined in the typology—or may not derive from them at all.

⁷ For example: Electrum, MyEtherWallet, MetaMask, Ledger, Trezor cryptoasset trading platforms.

⁸ For details, see also "Typology of Money Laundering Through Casinos", Chapter 3, Section F.1 (Money Laundering Methods Through Fixed-Game Gambling).