

Analysis

On Trends of Money Laundering from Card Fraud

Card fraud¹ involves the unauthorized acquisition and misuse of another person's bank card or equivalent payment instrument information for financial gain. Fraudsters may deceive cardholders into providing consent for transactions or they may carry out unauthorized transactions on the cardholders' accounts.

According to an October 2021 report by the European Central Bank, losses due to card fraud accounted for 3,6% of total transaction volume, with more than half of these fraudulent transactions occurring in **cross-border operations**².

A 2022 study by the European Association for Secure Transactions (EAST) further revealed that a significant portion of card fraud cases involve the use of **advanced technological methods**³. Criminals commonly obtain card details through phishing attacks or similar schemes, using the stolen information to make unauthorized transfers to accounts they control or to make payments on online platforms.

An analysis of card fraud cases in the Republic of Armenia indicates that a prevalent method involves fraudsters impersonating financial institution employees or government representatives. **Through phone calls or online interactions**, they convince victims to disclose their bank card details, e-wallet credentials, transaction confirmation codes, and other sensitive information⁴. Victims, believing they are securing a loan, government financial aid, or other financial benefits, voluntarily provide access to their accounts. This enables criminals to steal funds from bank accounts and e-wallets. In some cases, fraudsters use the victim's stolen e-wallet access to apply for loans under their name and embezzle the disbursed funds.

¹ Card fraud may take the form of theft using computer technology, fraud, or other criminal offenses.

² European Central Bank, "Seventh report on card fraud" (2021), <http://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html#toc6>

³ EAST, "Fraud Update 1-2022" March 2022 (<http://www.association-secure-transactions.eu/east-publishes-fraud-update-1-2022/>), EAST, "Fraud Update 2-2022" July 2022 (<http://www.association-secure-transactions.eu/east-publishes-fraud-update-2-2022/>)

⁴ "Cyber theft and money laundering case goes to court", 07.09.2022, <http://www.investigative.am/news/view/hamakargchayin-hapshtakutyun-poxeri-lvacum.html>.

"The preliminary investigation into a separate part of the case involving the theft of funds using computer technology has been completed", 05.01.2022, <http://www.investigative.am/news/view/hamakargchi-mijocov-hapshtakutyun1.html>.

"The preliminary investigation into the case of cyber theft from over twenty individuals and financial institutions has been completed", 14.10.2022, <http://www.investigative.am/news/view/hapshtakutyun-erku-tasnyakic-avel-andzancic-avart.html>.

Criminal investigations have also uncovered fraudsters creating **fake websites that mimic legitimate businesses**, including online gambling platforms⁵. Victims enter their real long credentials on these counterfeit sites, unknowingly granting access to criminals. The fraudsters then access the victims' actual accounts and transfer funds to their personal accounts or use them for online purchases.

Analysis of suspicious transaction reports conducted by the Financial Monitoring Center of the Central Bank of Armenia shows that individuals who gain unauthorized access to bank card data often exploit **cashless payment systems used by merchants and service providers** to launder illicit funds. With the rapid development of technology and online commerce, there has been an increase in the use of virtual POS terminals⁶. Fraudsters take advantage of this by registering legal entities or individual entrepreneur accounts solely to obtain virtual POS terminals, without engaging in actual business activities. These virtual POS systems allow them to process transactions using stolen card details, disguising illicit funds as legitimate business revenue. As a result, stolen funds appear as customer payments to businesses, making them less suspicious at first glance within the financial system.

The following indicators may suggest the illegal use of bank card or equivalent payment instrument information for the misappropriation of funds or attempts to legitimize stolen funds:

- Shortly after logging into an e-wallet from a new device, the user conducts transactions significantly exceeding their typical transaction amounts and/or applies for a loan. Shortly after the wallet is replenished, the funds are either withdrawn in cash or transferred to other wallets/bank accounts.
- After logging into a personal account on an online gambling website from a new device, the account is funded with an unusually large amount inconsistent with the customer's gambling behavior. Shortly after funding the gambling account, the funds are transferred to another gambling account, withdrawn in cash, or transferred to other wallets/bank accounts.
- Large amounts of money are deposited into the customer's bank accounts from multiple foreign cards and the nature of the transactions does not align with the customer's business profile. The customer quickly withdraws the received funds in cash or transfers them to other wallets/bank accounts.

⁵ "The preliminary investigation into the case of cyber theft and the unlawful acquisition of access to computer information has been completed", 04.07.2022, <http://www.investigative.am/news/view/hapshtakutyun-hamakargchayin-texnikayi-gorcadrmamb.html>.

⁶ POS terminals are devices used at points of sale to accept cashless payments. Virtual POS terminals are electronic solutions integrated into a merchant's website, enabling customers to make online purchases from that merchant.

- Transfers received from foreign cards into the customer's bank accounts are frequently reversed by the sender.
- The customer's bank accounts receive transfers from cards that have been reported as lost or stolen.