THE MISUSE OF INTERNET AND MOBILE PAYMENT SYSTEMS FOR MONEY LAUNDERING (ML) AND TERRORIST FINANCING (TF)

CFATF Research Desk

December 19th, 2023

INTRODUCTION

This final article of the "Emerging Trends" series will examine how criminals use online payment systems and mobile money for money laundering (ML) and terrorist financing (TF) purposes.

KEY DEFINITIONS

Internet Payment Systems

- These are internet-based mechanisms for customers to access pre-funded accounts, which customers can use to transfer electronic money or value held in those accounts to other individuals or businesses (FATF 2013, p. 9).
- The recipient redeems the value from the issuer by making payments or withdrawing the funds. Withdrawals occur by transferring the funds to a regular bank account, a prepaid card, or another money or value transfer service.
- Customers can also fund their accounts via bank transfers, payment card accounts or other funding sources.
- The most widely used Internet or online payment systems are electronic payment cards (debit, credit, and charge cards), e-wallets, virtual credit cards, and stored-value card payments.

KEY DEFINITIONS

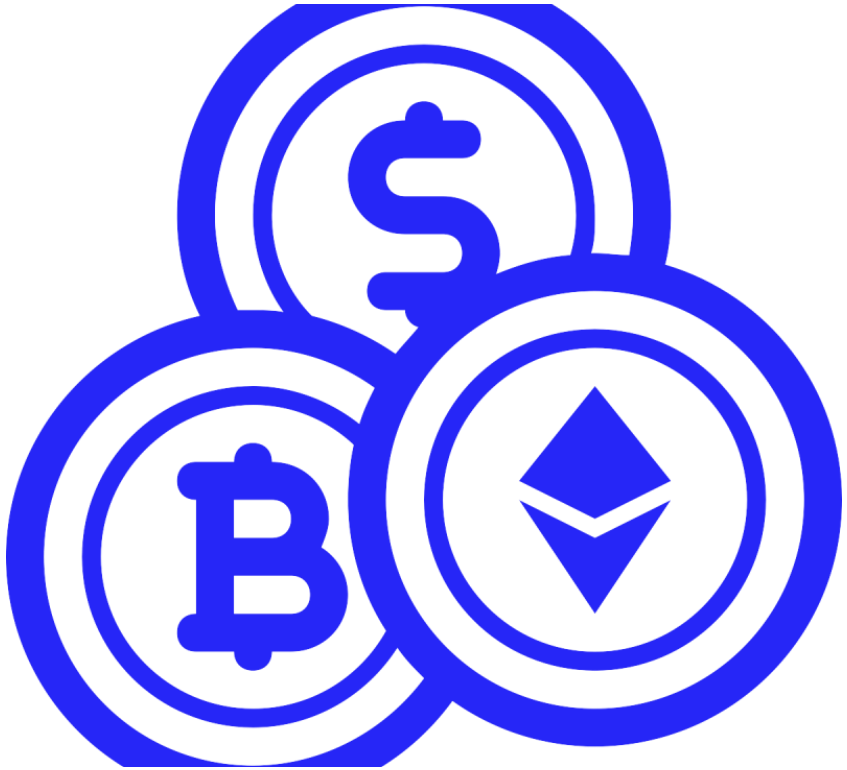
Mobile Payment Systems

- These are payments made through wireless devices like mobile phones and smartphones.
- Financial institutions facilitate mobile payments, including person-to-business (P2B), person-to-person (P2P) or government-to-person (G2P) transactions, which can be traditional payment service providers (banks or depository institutions) or non-bank payment service providers, such as money value transfer services (MVTS) (Bezhovski 2016, p. 128; FATF 2013, p. 7).

KEY DEFINITIONS

Virtual Asset Service Providers (VASPs)

VASPs can also utilise online platform-based exchanges or mobile apps for making payments or transferring funds globally through different payment channels, such as open and closed-loop systems, systems intended to facilitate micro-payments or government-to-person/person-to-government payments (FATF 209, ps. 12-13).



ML/TF RISKS: INTERNET AND MOBILE PAYMENT SYSTEMS

Misusing online payment systems and mobile money for ML/TF is a growing challenge. Here are some ML/TF risks these platforms can be exposed to:

Increased Anonymity: These payment systems can allow for non-face-to-face business relationships, which may enhance the risks of identifying fraud or the purposeful use of inaccurate information to conceal illicit activities.

Since criminals can move funds almost instantaneously worldwide, it may become more difficult to trace funds, the users and entities involved in transactions (FATF 2013, p. 14). In some cases, funding a payment method can be done through channels that are not regulated or used by an unknown third party, increasing the ML/TF risks.

VA products or services can utilise technology that facilitates pseudonymous or anonymity-enhanced transactions that hinder the efforts that track and identify the parties involved (FATF 2013, p. 16; FATF 2019, p.11).

ML/TF RISKS: INTERNET AND MOBILE PAYMENT SYSTEMS

Virtual Asset Transactions: Related to the previous point, using cryptocurrencies, digital currencies, and other virtual assets in online payment systems can add an extra layer of anonymity, making it challenging for authorities to track and identify the individuals involved in the transactions.

Moreover, the global reach and transaction speed of VAs as mechanisms for online and mobile payment systems make it easier for illicit actors to move funds across jurisdictions quickly, complicating efforts to coordinate international regulatory responses.

ML/TF RISKS: INTERNET AND MOBILE PAYMENT SYSTEMS

Layering and Integration: Perpetrators may use multiple and complex transactions and accounts to make it difficult to pinpoint the origin of funds. These transactions can involve multiple transfers between online accounts, making it difficult to trace the source of the funds.

Criminals usually achieve this by opening several accounts based on false documents and transferring funds without the knowledge of the person whose documents were falsified (Matejić and Ćurčić 2022, p. 224).

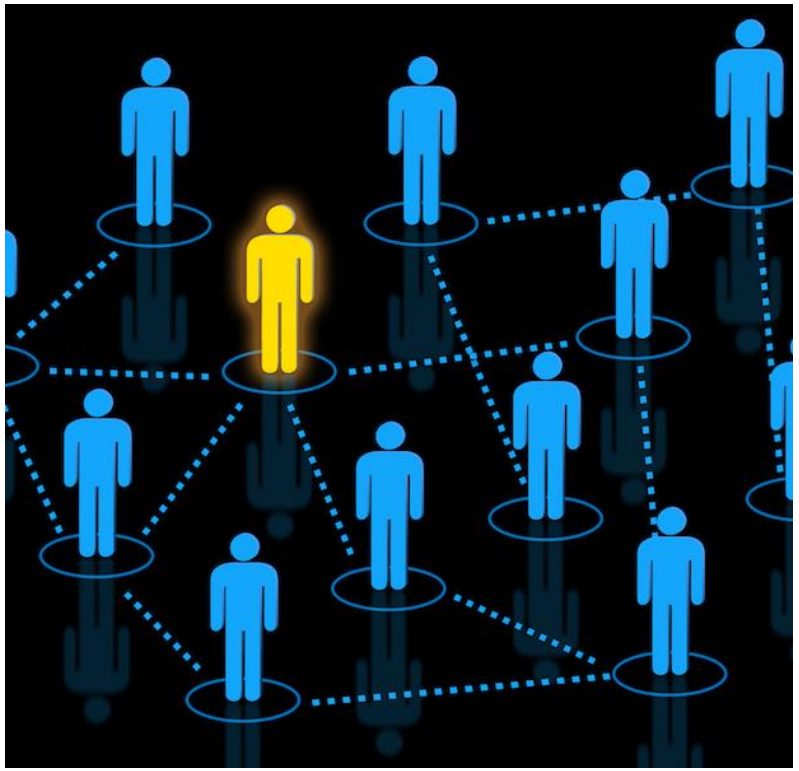
ML/TF RISKS: INTERNET AND MOBILE PAYMENT SYSTEMS

Smurf Accounts: Criminals may employ smurfing and structuring schemes to circumvent the thresholds and suspicious reporting requirements (FATF 2013, p. 28). Criminals make smaller payments from multiple accounts through a mobile or online banking application.

Trade-Based Money Laundering: New technologies and the digitalisation of trade allow for an increased speed of trade operations (FATF 2020, p. 38). However, criminals may use online payment systems to engage in international trade transactions to manipulate invoices or misrepresent the value of goods and services, facilitating the movement of illicit funds across borders.

ML/TF RISKS: INTERNET AND MOBILE PAYMENT SYSTEMS

Peer-to-Peer Transactions: Internet and mobile payment services often allow peer-to-peer transactions, and criminals may exploit this feature to move illicit funds between accounts without the need for traditional banking channels which have established KYC and CDD measures.



MEASURES TO MITIGATE THE ML/TF RISKS

The private sector, regulatory bodies, and financial institutions play a crucial role in implementing and enforcing robust AML/CFT measures to establish proportionate and risk-based measures to prevent the misuse of online and mobile payment systems.

Customer Due Diligence: providers should take measures to identify and verify customers' identity, which will vary depending on the level of risk the product poses. Non-face-to-face verification of customer identity often requires corroborating information received from the customer with information in third-party databases or other reliable sources. Transaction monitoring and suspicious activity reporting are also essential.

MEASURES TO MITIGATE THE ML/TF RISKS

Source of funding: An anonymous or unregulated source of increased ML/TF risk and restrictions should be in place to prevent these funds from accessing payment channels.

Record keeping, transaction monitoring and reporting: Transaction and CDD records are key to AML/CFT efforts and support law enforcement investigations. At a minimum, the transaction record of a payment or funds transfer should include information identifying the parties to the transaction, any account(s) involved, the nature and date of the transaction, and the amount transferred.

MEASURES TO MITIGATE THE ML/TF RISKS

Allocation of Increased Supervisory Resources for Higher Risk Areas: As VASPs have attributes that would place them at higher risks, such as the use of anonymising technology, facilitating virtual-to-virtual financial activities or operating in higher-risk areas, supervisors should conduct the appropriate offsite and onsite supervision or monitoring and assessment to evaluate the adequacy of VASPs' policies and procedures.

REFERENCES

- Bezhovski, Zlatko (2016), The Future of the Mobile Payment as Electronic Payment System, European Journal of Business and Management, vol. 8, number 8.
- FATF (2013), Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments And Internet-Based Payment Services, FATF, Paris.
- FATF (2019), Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris.
- FATF – Egmont Group (2020), Trade-based Money Laundering: Trends and Developments, FATF, Paris, France.
- Matejić, Ivica and Ćurčić, Mihailo (2022), The Role of Electronic Payments in Money Laundering, Security Challenges Of Modern Society: Dilemmas and implications Thematic International Monograph, Belgrade.

We hope that you found the "Emerging Trends" series informative and interesting.

1-868-623-9667

cfatf@cfatf.org

www.cfatf-gafic.org