ST. KITTS BRANCH
Financial SERVICES Regulatory Commission

NewsLetter

February 2024
Issue No. 116

The Misuse of Internet and Mobile Payment Systems for Money Laundering, Terrorist Financing & Proliferation Financing

IN THIS MONTH'S ISSSUE:

- ⇒ **Internet & Mobile Payment Systems and their key components**
- ⇒ **ML/TF/PF Risks associated with Internet and Mobile Payment System**
- ⇒ **Measures to Mitigate the ML/TF/PF Risks**
- ⇒ **Case Study**

Internet Payment System

An internet payment system, also known as an online payment system or an electronic payment system, refers to a mechanism that allows individuals and businesses to conduct financial transactions over the internet. This system facilitates the exchange of money electronically, enabling users to pay for goods and services, transfer funds or conduct other financial transactions through online payments.

Key components of an internet payment system include but are not limited to:

1. Payment Gateways;
2. Merchant Accounts;
3. Digital Wallets;
4. Credit/Debit Cards;
5. Bank transfers; and
6. Cryptocurrencies.

Popular internet payment systems include Paypal, Stripe, Square and other various region-specific systems. These systems have played a crucial role in the growth of e-commerce and the digitization of financial transactions.

Mobile Payment System

A mobile payment system refers to technology that enables users to manage financial transactions using a mobile device such as a smartphone or tablet. This system leverages wireless communication technologies to facilitate the transfer of funds and complete various financial transactions.

Key components of mobile payment systems include the following:

1. Mobile wallets or Digital wallets;
2. Mobile Banking Apps;
3. Short Messaging Service Based Payments;
4. Near field Communication;
5. Quick Response Code Payments; and
6. In-app Payments.

Mobile payment systems play a significant role in transforming traditional payment methods and contributing to the growth of the digital economy.

Internet and mobile payments systems can be vulnerable to Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) activities due to the nature of these systems and the potential for criminals to exploit certain weaknesses.

The following are ML/TF/PF risks associated with internet and mobile payment systems:

1. Anonymity and Pseudonymity:

- **Digital Currencies and Cryptocurrencies** - The use of digital currencies such as Bitcoin and other cryptocurrencies, can further complicate efforts to trace financial transactions due to the decentralized and pseudo-anonymous nature of these systems.
- Prepaid cards and virtual wallets can be used to store and transfer funds without the need for traditional banking channels which provide an avenue for illicit financial activities.

2. Cross-Border Transactions:

- **Global Nature of Transactions** - Internet and mobile payment systems facilitate cross-border transactions. The global nature of these systems make it difficult for regulatory agencies to monitor and regulate transactions effectively.
- **Complex Payment Flows** - Illicit characters may exploit the complexity of cross-border transactions to disguise the origin and destination of funds making it difficult to identify suspicious activities.

3. Peer-to-Peer Transactions:

- **Decentralization** - The use of peer-to-peer (P2P) payment systems can facilitate direct transaction between individuals without the need for intermediaries. This can be exploited for illegal transfers without detection.

4. Insufficient Know Your Customer (KYC) Measures:

- **Weak Customer Verification** - Some payment systems may have weak, limited or no KYC procedures which allows individuals to open accounts with minimal or fraudulent documentation. The lack of a robust verification system can enable money launderers, terrorists and proliferation financiers to exploit the system.

5. Mobile Device Vulnerabilities:

- **Security Risks** - Mobile devices are susceptible to various security risks such as malware and phishing attacks. If a user's mobile device is compromised, attackers may gain unauthorized access to payment apps and conduct illicit transactions.

6. Layering and Transaction Smurfing:

- Money launderers often engage in layering, which involves complex transactions designed to obscure the origin of funds. This can include breaking down large amounts into smaller transactions (transaction smurfing also known as structuring);

7. Integration of Legitimate and Illegitimate Funds:

- Criminals may use online payment systems to mix illicit funds with legitimate ones, making it harder for authorities to differentiate between legal and illegal transactions.

8. Use of Mules:

- Criminals may recruit individuals as money mules to facilitate the movement of funds. Mules may unknowingly or knowingly assist in transferring money through online payment systems which can be used to assist in ML,TF and PF activities.

9. False Transactions and Shell Companies:

- Criminals may create false transactions or set up shell companies to legitimize the source of funds using online payment systems to give a façade of the legitimacy of their activities.
- Efforts to combat the misuse of internet and mobile payments for ML, TF and PF involve a combination of regulatory measures, enhanced due diligence by financial institutions and payment service providers, international cooperation and adoption of advance technologies for monitoring and detecting suspicious transactions .

Mitigating ML/TF/PF risks in internet and mobile payment systems involves implementing a comprehensive set of measures aimed at enhancing security, transparency and regulatory compliance.

Key measures to mitigate ML/TF/PF risks:

1. Robust KYC Procedures;
2. Enhanced Due Diligence for High-Risk Transactions and Persons;
3. Transaction Monitoring Systems;
4. AML/CFT/CPF Compliance Training;
5. Secure Mobile Applications;
6. Regulatory Compliance;
7. Customer Due Diligence for Third-Party Providers and Intermediaries;
8. Transparent Transaction Records;
9. Collaborating and Information Sharing;
10. Implementing Internal Controls and Governance; and
11. Establishing Risk Assessment procedures.

Kindly refer to the FSRC's prior Newsletter Editions on the following related topics:

- ***November 2023, issue No. 113 - Don't be a Mule : All about Money Mules***
- ***October 2023, Issue No. 112 - The Role of Shell Companies in Money Laundering***
- ***May 2021, Issue No. 84 - Virtual Assets: Vehicle for Financial Crime***
- ***March 2021, Issue No. 83 - Detecting & Preventing the Illicit Cross-Boarder Transportation of Cash and Bear Negotiable Instruments (BNIs)***

CASE STUDY

Suspected Use of Open-Loop Cards and Online Payment Systems to Launder Drugs

This case was generated following the receipt of information from a foreign Financial Intelligence Unit (FIU) which indicated that a number of individuals were charged for laundering millions of drug proceeds through a company providing open-loop cards in Country A. The funds were suspected to be loaded on prepaid cards and moved, for example, from Country A to South America. Other criminal activities were also suspected to be the source of the illicit funds.

Two of the individuals, associated with the prepaid card company, were found to have addresses in both Country A and Canada and had opened bank accounts and established at least one Company in Canada. The bank accounts in Country A and in Canada were used to receive funds from various individuals and entities located in several different countries in Central America, Europe, Africa, Asia as well as Country A and Canada.

It was further revealed that two (2) Canadian Internet Payment System providers (IPS) sent funds to the same prepaid card company in Country A. Based on available information, it appeared that both of the IPS offered a prepaid service to their clients, which was provided by the prepaid card Company A.

One of the Canadian IPS was the subject of another case in which it was suspected of facilitating the Laundering of Ponzi scheme proceeds.

Suspicious transactions included third-party cash deposits and International electronic funds transfers (EFTs). Most of the funds received in the Canadian accounts were transferred back to the accounts held in Country A by the prepaid card company and two associated companies in Country A.

Red Flags identified:

1. Cross-Border movement of prepaid cards was involved, as the funds were withdrawn from the card in a jurisdiction different from where the cards had been loaded.
2. A large number of bank accounts held by the same prepaid card company were used as flow-through accounts which is indicative of layering activity.

Reference:

CFATF Research Desk—December 2023 & FATF Report

South Independence Square Street, P.O. Box 898, Basseterre, St. Kitts
Tel: (869) 466-5048 | 467-1019/1591
Website: www.fsrc.kn / Email: info@fsrc.kn