FINANCIAL INTELLIGENCE UNIT - GUYANA

Typology Report

Account Takeover - Mobile Payment Service

September 2025

TABLE OF CONTENTS

ACCOUNT TAKEOVER – MOBILE PAYMENT SERVICE

OVERVIEW

The Financial Intelligence Unit (FIU)- Guyana is publishing this typology in keeping with its mandate of conducting strategic analysis[1] to identify and inform the public on existing and emerging money laundering (ML), terrorist financing (TF) and proliferation financing (PF) related trends and patterns. A typology refers to the systematic classification of various ML/TF/PF schemes that appear to be constructed in a similar fashion or using similar methods.

This information is used by the FIU or other state agencies to determine ML/TF/PF related threats and vulnerabilities, and understand the methods used by criminals to commit these types of financial crimes. Strategic analysis may also help in the development of risk-based strategies and action plans for policy makers, more specifically, regulatory bodies within the Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT)/Combatting Proliferation Financing (CPF) framework of Guyana.

PURPOSE

This typology report seeks to bring awareness to reporting entities, supervisory authorities, other competent authorities and the public, to the potential ML/TF risks that are possible through fraud committed via mobile payment services. More particularly, it aims to provide information on scammers' use of social engineering to gain control of the accounts of mobile payment service users and defraud these unsuspecting victims of their funds.

The report also provides key red flags or indicators related to this category of fraud and offers recommendations that may be considered by the target audience, in the formulation of best practices, policies, procedures and controls, to mitigate these risks and ensure protection of their systems or themselves, from criminals and/or criminal enterprises. By understanding these risks and indicators, reporting entities can improve the detection and reporting of suspicious activity. The public will also be able to better safeguard themselves from becoming victims, which will altogether support Guyana's efforts to combat financial crime.

[1] As part of its commitment to fulfil international obligations under Financial Action Task Force (FATF) Recommendation 29 and in keeping with Section 9 of the AML/CFT Act 2009.

BACKGROUND

Across the world, mobile money services are growing rapidly as public trust in this system of payments continues to expand. Mobile-based money transfers are intended to enhance financial inclusion, by facilitating easy deposits, withdrawals and payment for goods and services using a mobile device. In some cases, the services are extended to include micro lending/ credit opportunities. However, as the mobile money ecosystem has evolved, so have the risks of fraud, when using these services. Those with ulterior motives have targeted mobile money service providers and users, to steal personal information and money. Fraudulent activities are conducted using methods like mobile application (app) fraud, SIM swap fraud, account takeovers, and social media scams, which present significant challenges for detection and prevention for the industry and users alike. As outlined above, this typology will focus on mobile money fraud involving **account takeovers**.

Without prejudice, the legal definition of 'Fraud' under the Criminal Law Offences Act or Common Law, classifies fraud as a financial crime in the broader financial services context. The AML/CFT Act 2009 specifically lists, in the Second Schedule, the offence of "fraud" among the serious or predicate offences that are linked to ML or TF. In this context, the GSM Association (GSMA)[2] defines 'mobile money fraud' as an act or situation where a person or an entity dishonestly makes a false representation by abusing position or technology, with the intent to financially gain or cause loss to another person or entity.

False representation, commonly referred to as social engineering, is widely used to initiate fraud in mobile money services. Social engineering takes advantage of a potential victim's natural tendencies and emotional reactions. It uses psychological manipulation to trick users into making security mistakes or unwittingly disclosing sensitive information, which allows the scammers to access the accounts of their victims. This information is then used or shared for fraudulent purposes. It is therefore imperative that regulated entities, other organizations and individuals be aware of the potential risks of this type of fraud and adopt mitigating measures to protect themselves from financial losses.

[2] A non-profit trade association that represents the interest of mobile network operators worldwide.

TYPOLOGY:

ACCOUNT TAKEOVER – MOBILE PAYMENT SERVICE

A review of the Suspicious Transaction Reports (STRs) for 2024 noted an increasing trend of fraud against the customers and accounts of payment service providers (PSPs), by way of account takeovers.

HOW DOES THIS SCAM WORK?

This multi-stage fraud scheme involves two stages:

1. Use of **social engineering via pretexting** - to obtain the victim's mobile account information; and
2. Conducting **account takeovers** – to gain unauthorized control of the victim's mobile account.

Further descriptions of what these two stages entail along with relevant case studies are presented below.

Stage 1: Social engineering

This involves an act of pretending to be another (real or non-existent, and/or representing an entity), to manipulate someone into divulging personal or private information, thereby unwittingly granting access, or performing certain actions leading to fraud. This type of fraud involves ***impersonation and deception.*** The person or entity that the scammer is purporting to be or represent can be genuine, fictitious, or created using a blend of genuine and/or fictitious information. In the context of mobile money fraud, scammers usually pretend to be employees or agents of the PSP, or staff of other organizations often utilizing pretexting, in order to gain the victim's trust.

For this typology being presented, ***pretexting*** was identified as the form of social engineering attack utilized by scammers locally to defraud their victims. It involves the creation of a situation (fictious information) that convinces the victim to reveal personal or private information. The scammer will pretend to be someone legitimate or familiar to cause the victim to feel comfortable, e.g. a customer service agent or someone from the PSP's system support team. During pretexting attacks, scammers

typically ask victims for certain information, on the backdrop of the false scenario/narrative presented. In reality, the scammer steals this information and then uses it to carry out secondary attacks. In addition, criminals can sometimes go as far as mining or researching information about the victim beforehand, to make the scam seem more believable.

Case Study: Pretexting

The case study below presents a summary of pretexting methods employed by scammers locally:

Stage 1: **Pretexting**

- Scammers may **retrieve data available on intended victim** via public sources e.g. name, phone number, email address, etc.
- Scammer contacts the intended victim (in some cases representatives of the account holder) via phone/WhatsApp, ***impersonating staff*** of known PSPs.
- ***Purports issues with victim's account* or *promises new added benefits.*** These issues may include:

  Locked accounts, compromised/hacked accounts, account deletion due to dormancy, required account upgrade and need for opening of new accounts to get added incentives.

  Note: Scammers can simultaneously entice the victim with reasons why addressing the fictitious issues above will be beneficial. These include *Opportunities for earning larger commissions, benefiting from a new/ better user experience and fake promotional winnings for crediting account.*
- Employs different techniques to ***appear legitimate*** and gain victim's trust such as:

  Fake mobile application links, dashboards and switchboard recordings, use of spoof emails and possessing and confirming personal information of the victim.
- ***Convinces victim to provide account credentials/other personal information*** to resolve issues or perform upgrades. These include access codes and one-time passwords (OTPs).

Stage 2: Account Takeover

This is the **unauthorized access and control** over a legitimate mobile money user's account/wallet. It may involve exploiting vulnerabilities in the account security measures, such as weak passwords, poor authentication procedures, or social engineering tactics, to gain unauthorized access to the

account. An example of this activity is when acquired account information is used to attempt to bypass security measures, which may include PINs, passwords, and security questions to access the victim's account. As mentioned above, pretexting was observed as the tactic mostly employed locally to gain unauthorized access and control of victims' accounts. When inside the account, the fraudster can complete unauthorized transactions, transfer funds to other accounts (including their own), or even withdraw money through mobile money agents. In some cases, the fraudster changes the account settings, such as the user's personal information, to hinder the victim's ability to regain control and receive notifications about account activities.

Case Study: Account Takeover

The case study below presents a summary of account takeover methodologies utilized by scammers locally:

Stage 2: **Account Takeover**

- ***Scammer Gains access*** to the victim's account/wallet via pretexting.
- ***Changes victim's credentials*** i.e. password and email (with the help of the victim by requesting OTPs).

  Note: At this point, *scammers usually request the victim to restart/turn off their mobile device*. This results in the victim missing important notifications (SMS/other) regarding their account activities.
- Once changed, the ***victim no longer has authority/access*** to their account.
- ***Scammer conducts one or a series of fraudulent transactions/unauthorized transfers*** thereby depleting funds in the account.

  Note: Here the scammer seeks to immediately isolate/withdraw the stolen funds by:
  - ✓ *Transferring funds to account(s) known/controlled by the scammer;*
  - ✓ *Transferring funds to agent accounts to conduct cash-outs (often facilitated through third parties);*
  - ✓ *Conducting other transactions such as top-up purchases, funding data plans and purchase of goods/services via online merchants; and*
  - ✓ *Making payments towards the processing of anonymous transactions e.g. anonymous betting vouchers.*
- Scammer can ***no longer be contacted.***

RED FLAG INDICATORS:

- ✓ Being provided links to fake/non-functional mobile payment applications.
- ✓ Being requested to urgently credit mobile payment accounts.
- ✓ Being requested to turn off cellular device or ignore SMS/other notifications.
- ✓ Being requested to provide/confirm account credentials including OTPs.
- ✓ Being requested to change personal account information.
- ✓ Being contacted via fake/unofficial email addresses/telephone numbers.
- ✓ Use of high-pressure tactics (including threat of account deletion) and a sense of urgency to credit accounts.
- ✓ Receiving unsolicited calls from someone in "tech support" about a problem that requires your immediate attention.

HOW CAN USERS STAY PROTECTED?

- ✓ Immediately contact your PSP upon suspicion of scams.
- ✓ Stay educated - verify information through official channels (social media pages, websites, known contact numbers, etc.).
- ✓ Pay keen attention to SMS/other notifications regarding account activities.
- ✓ Protect account credentials including OTPs.
- ✓ Ensure that other trusted parties/representatives with access and control to your mobile money account are sensitized.

RECOMMENDATIONS

REPORTING ENTITIES:

The following recommendations are suggested for better system safeguard against account takeovers:

- ✓ Conducting regular AML/CFT risk assessments of mobile payment systems to identify fraud-related vulnerabilities and implementing measures to address specific risks;
- ✓ Implementing 'privacy by design' (integrated into products, services, and system designs by default) and/ or best practice cybersecurity frameworks to strengthen systems to act as a barrier to account takeovers, and by extension, other types of frauds;
- ✓ Developing comprehensive AML/CFT programs, including anti-fraud programs that include red flags /indicators to aid in the detection of suspicious activities; and cooperate with law enforcement agencies with their investigation and response strategies to this type of fraud;
- ✓ When possible, invest in advanced technology such as artificial intelligence and machine learning for improved AML/CFT lines of defense, including for fraud detection and adapting systems to manage evolving fraud schemes;
- ✓ Establishing clear profiles for users/agents to identify unusual or fraudulent requests. All changes to normal user instructions should be appropriately verified, and if necessary, the user profile updated;
- ✓ Proactively educating customer facing staff on the ML/TF risks associated with 'users/agents' and the latest techniques being used by fraudsters to steal their personal information so that they remain alert;
- ✓ Where applicable, raising awareness and sensitizing users/agents on the protection of personal information (including name, address, passwords, etc.) should become routine practice, e.g. through SMS reminders, warning notices at agent locations, etc.;
- ✓ Where applicable, informing users/agents on responses to compromised personal information e.g. immediately contacting the PSP and reporting the matter to law enforcement authorities;

- ✓ Creating robust user recourse and escalation procedure to ensure internal and external reporting of STRs to the FIU;
- ✓ Warranting employee and agent screening, training, testing and routine monitoring to ensure that they don't unwittingly release users' personal information or tip off a customer who is the subject of a STR;
- ✓ Conducting management review of high-value transactions; and more importantly pay special attention to complex, large or unusual transactions to determine whether a transaction is suspicious or requires escalation through the reporting channel;
- ✓ Subject to applicable laws or legal obligations, determine whether to immediately terminate/freeze accounts of known scammers and report matter immediately to the relevant law enforcement authority to enable the application of applicable freezing and / or recovery measures with respect to the proceeds of illegally obtained funds or property;
- ✓ Reporting suspected scammers immediately to law enforcement agencies and filing STRs with the FIU; and
- ✓ Providers (reporting entities) can participate in national awareness programs and /or jointly hold capacity building and training in collaboration with FIU, law enforcement agencies to enable them to deal with ML, TF, other financial crimes including fraud incidents promptly.

SUPERVISORS/OTHER COMPETENT AUTHORITIES:

Given the dynamic nature of mobile money and the growing threat of fraud in this industry, it is crucial for both supervisors and law enforcement to consider the following recommendations:

- ✓ Issuing guidelines to reporting entities and developing standard operating procedures that require mobile PSPs to design and implement effective AML/CFT programs including in relation to anti-fraud controls;
- ✓ Documenting and providing feedback to the AML/CFT/PF Committee for enhancing AML/CFT and related laws to address specific nuances or deficiencies observed in the laws relating to mobile money fraud. This will ensure laws and regulations are robust enough to detect, prevent, prosecute and recover illicit proceeds from such cases effectively;

- ✓ Ensuring PSPs conduct ongoing monitoring of user/agent activities and strengthen their ability to effect and comply with customer due diligence requirements;
- ✓ Providing technical training and resources, including for AML/CFT purposes, to deepen understanding and build technical capacity to support stakeholders in detecting, preventing and managing mobile money fraud;
- ✓ Conducting periodic ML/TF/PF risk assessments of mobile PSPs to systematically identify, analyze, and evaluate potential risks that could negatively impact financial entities and the broader financial system; and
- ✓ Ensuring inter-agency cooperation by bringing together various stakeholders to collaborate on various preventative measures, including awareness programs and information sharing.

REMINDER:

Reporting entities are reminded to be vigilant and where there is a suspicion of ML/TF /PF activities, proceeds of crime, associated predicate offence, a suspicious transaction report **MUST** be filed with the FIU.

Further, if you believe that the information is serious and requires an immediate law enforcement response, then you should contact the Criminal Investigation Department of the Guyana Police Force.

CONCLUSION

As mobile payment service gains widespread acceptance and trust among users, criminals adapt and find strategies for exploiting the mobile money space for illicit gains. A proactive, intelligence-led collaborative approach is therefore essential to detect and close loopholes, preventing illicit financial flows, and maintaining the integrity of this sector. FIU-Guyana will continue to play its part in sharing information and providing guidance and feedback to reporting entities, supervisory authorities and other competent authorities through strategic insights, typologies, and indicators to enhance detection and compliance with legal and regulatory obligations.

The mobile payment service sector remains a valuable but potentially vulnerable sector and primary target for fraud and ML, due to its rapid growth, ability to facilitate speedy transfers, relative transaction anonymity, etc. In addition, the lack of awareness and understanding among many users, and the absence of strong payment security measures for some mobile payment systems, have added to the sector's susceptibility to fraud.

To assess, manage and mitigate these risks, all stakeholders including PSPs and users must remain vigilant in identifying red flags and suspicious patterns. Strengthening AML/CTF controls and operational security measures, enhancing transaction monitoring, and fostering a culture of compliance is essential to ensure the safeguarding of Guyana's mobile payment service sector from ML/TF and other related financial crimes.