FINANCIAL INTELLIGENCE UNIT - GUYANA

Typology Report

Online Sales/Non-Delivery Scam - Mobile Payment Service

September 2025

TABLE OF CONTENTS

ONLINE SALES/NON-DELIVERY SCAM – 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, 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 the internet/social media to defraud unsuspecting shoppers of their funds.

The report also provides key 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 ultimately 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 grow. 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 increased 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 **online sales/non-delivery scam**.

Fraud is defined as 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. The GSM Association (GSMA)[2] defines mobile money fraud as a person or an entity dishonestly making a false representation by abusing position or technology, with the intent to financially gain or cause loss to another person or entity.

False representation is often presented in the form of impersonation, which is widely used to initiate fraud in mobile money. When coupled with the use of online platforms, this combo can be utilized as a lucrative methodology by scammers to lure unsuspecting victims into sending them funds. Hence, while the internet has connected people to more information, today's digital age has made it easier for scammers to perpetrate their fraudulent activity. From faux social media postings to password phishing for financial accounts, scammers have found numerous ways to get their hands on other peoples' money. Therefore, it is imperative that individuals and organizations be aware of the potential risks of this type of fraud and adopt mitigating measures to safeguard themselves and their entities respectively, from significant financial losses.

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

TYPOLOGY:
ONLINE SALES/NON-DELIVERY SCAM – MOBILE PAYMENT SERVICE

While most online sellers are legitimate, unfortunately, scammers use the anonymous nature of the internet to defraud unsuspecting shoppers. Strategic analysis conducted by the FIU-Guyana has revealed a trend of fraud involving the use of **online platforms** and **mobile payment accounts**. This type of fraud – referred to as 'Online Sales/Non-Delivery Scam' is a type of advance fee fraud whereby scammers elicit an advance payment for the sale of a good or a service, but that good or service is never delivered to the intended customer (victim). Here, the scammer leverages the anonymity and reach of online platforms, and the reach of mobile money agents to target potential victims.

WHAT DOES THIS SCAM INVOLVE?

Impersonation

It involves the act of pretending to be another person, real or non-existent, and/or representing an entity for the purpose of deceiving others. The person or entity the imposter is purporting to be or represent, can be genuine, fictitious, or created using a blend of genuine and/or fictitious information. Here, much emphasis is placed by the scammer in maintaining anonymity.

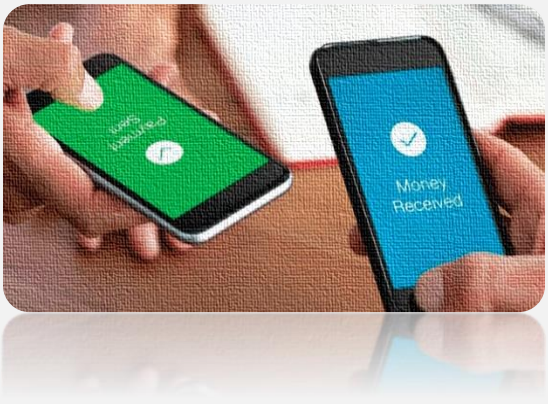
Online Platforms

Scams occur through online platforms such as social media to deceive others into sending money. For example, scammers put up fake advertisements involving the sale of fictitious merchandise/property or availability of a

fictitious service with the aim of tricking customers into sending money. The perpetrators use various platforms with the most frequently used platforms locally being Facebook Marketplace and Instagram. This methodology remains attractive for use by scammers since it removes the need for physical meetups, has a wide reach, inter alia.

Advance Fees

This simply involves requests by a seller/supplier for upfront payments/fees for advertised goods/services before they are delivered. In the context of this scam, victims pay upfront fees to the scammer in hopes of securing/receiving the advertised good/service.



Mobile Money Accounts

Mobile money accounts are often utilized by scammers when collecting advance fees from victims. These accounts can also be set up with fake identities, making recovery, arrests, and prosecution very difficult or impossible. Here the scammer leverages the anonymity, ability to facilitate quick transfers and wide reach associated with such accounts. This new technology has made it easier for perpetrators of advance-fee scams to alter their techniques and take advantage of more people in more ways.

HOW DOES THIS SCAM WORK?

The Diagram below presents a graphical representation of the methodology utilized by scammers locally in carrying out the Online Sales/Non-Delivery Scam:

Scammers impersonate other individuals/businesses or create fake profiles online through social media platforms e.g. Facebook Marketplace and TikTok.

Scammer advertises goods/services online using attractive prices and convincing descriptions to entice potential buyers.

After conversing with the scammers about the availability of the advertised goods/services, victims are then requested to provide upfront payment (advance fees) via mobile payment (to accounts often set up under false identities) on the guise of reserving/ordering/pre-ordering the required goods/services.

Once the victim makes the required payment, the scammers then immediately transfer/withdraw the funds.

Upon receipt of the funds, the scammers fail to deliver the promised goods/services or make excuses for non-delivery (such as late shipment/delivery of the purchased goods). Note: In some cases, additional fees may also be requested.

Scammers ultimately disappear and can no longer be contacted, leaving the victim without their purchased items/service and with lost funds.

RED FLAG INDICATORS:

- ✓ Providing **fake/ inadequate order confirmation** details.
- ✓ **Making requests for initial/ additional/ final payments** prior to delivery/ inspection of goods/ services.
- ✓ **Requesting mobile money transfers** for initial payment of goods/services.
- ✓ Offers advertised seem **too good to be true.**
- ✓ Use of **high-pressure tactics** and a **sense of urgency** (e.g. saying it's time-limited or they have other buyers interested) to receive payment in advance.
- ✓ **Shows unwillingness/ provides excuses** when asked to inspect goods/property.

HOW CAN USERS STAY PROTECTED?

- ✓ Be wary of goods/services with prices/features that are **too good to be true** – they probably are!
- ✓ **Don't pay** for goods/services **before physically inspecting/ receiving/ confirming their availability.**
- ✓ **Meet the seller in person,** if possible - so you can examine the goods before paying.
- ✓ **Do a little research on the seller** - always take the time to verify who you're talking to/ dealing with. Check the seller's profile for ratings, reviews, activity, and other listings.
- ✓ Immediately **contact your payment service provider/ police** upon suspicion of scams.

RECOMMENDATIONS

REPORTING ENTITIES:

The following are recommended to provide better protection against online sales/non-delivery scam:

- ✓ Develop comprehensive AML/CFT programs to aid in the detection and prevention of proceeds of financial crime and cooperate with law enforcement agencies in support of their investigation and response strategies, including in relation to these fraud schemes;

- ✓ Invest if possible, in advanced technology such as artificial intelligence and machine learning for improved financial crime (including fraud) detection, and implement systems to manage and mitigate the ML/TF risks evolving from these fraud schemes;

- ✓ Establish clear customer risk profiles for customers/ clients who are users/ agents to identify unusual or suspicious transactions, including suspected fraudulent requests;

- ✓ Keep up to date with public awareness or 'proactive education programs' developed for users/ agents and remain vigilant in relation to the latest techniques being used by scammers to steal money;

- ✓ Create robust user recourse and escalation procedures including but not limited to filing suspicious transaction/ activity reports with the FIU;

- ✓ Ensure adequate systems are in place to conduct independent AML/CFT Audits;

- ✓ Mandate and conduct management review for all high value transactions;

- ✓ Based on applicable legal provisions, determine whether to de-risk a customer, or immediately terminate/freeze accounts of known scammers; and

- ✓ Report suspected scammers immediately to law enforcement agencies and file suspicious transaction report with the FIU.

SUPERVISORS/OTHER COMPETENT AUTHORITIES:

Given the dynamic nature of mobile money and the growing threat of financial crimes including fraud schemes in this industry, it is recommended that both supervisors and law enforcement consider the following:

- ✓ Supervisory bodies should develop guidelines and provide related training on the ML/TF risks associated with mobile services and require providers to design and implement effective AML/CFT and anti-fraud controls;

- ✓ Supervisory bodies should ensure payment service providers conduct ongoing monitoring of user/agent activities and strengthen their ability to implement and comply with due diligence and other AML/CFT regulatory requirements;

- ✓ Law enforcement agencies and other relevant competent authorities should establish internal standard operating procedures (SOPs) to ensure quick and consistent response to reports or complaints received in relation to these fraud schemes;

- ✓ All relevant competent authorities should document and highlight legislative deficiencies or specific nuances in the laws governing the offences relating to mobile money fraud and share same with the AML/CFT/CPF National Coordinating Committee. This will aid in the enhancement of Guyana's legal frameworks by ensuring laws and regulations are robust enough to prosecute such cases effectively;

- ✓ All competent authorities and reporting entities should participate in technical training to deepen their understanding and build technical capacity to support stakeholders in detecting, preventing, reporting and managing mobile money fraud; and

- ✓ Participate fully in Guyana's ML/TF/PF National Risk Assessments, facilitate inter-agency cooperation and collaborate (where applicable) 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 or associated predicate offence being conducted with or via your entity, 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 may make a report to the Criminal Investigations Department of the Guyana Police Force (GPF).

CONCLUSION

The mobile payment service landscape has gained significant momentum locally and is expected to grow further in the coming years as Guyana's financial sector continues to expand. Payment service providers are seen as an extension of the formal and regulated financial sector, that allows for greater financial inclusion, especially for people in the lower income brackets of society. However, this service remains prone to attacks by bad actors seeking to exploit the inherent vulnerabilities of the system and of its users.

In this light, FIU-Guyana continues to develop, utilize and share intelligence with law enforcement agencies or relevant competent authorities and provide feedback on the quality of suspicious transaction reports to reporting entities. This is to aid in the detection of ML/TF/PF, proceeds of crime or associated predicate offences and close legal gaps as they may arise from time to time. These collaborative efforts serve to protect the public and the integrity of the local and international financial systems.

The mobile payment service sector by its nature is vulnerable and a target for criminals seeking to perpetuate fraud and other financial crimes, due to the system's ability to facilitate speedy transfers, maintain anonymity of users, inter alia. These features often work for the benefit of scammers carrying out their illicit acts. Moreover, the general lack of awareness and understanding of users often increases their susceptibility to fraud.

It is essential that these risks are effectively assessed, managed and /or be mitigated by all stakeholders including payment service providers and users. To achieve this, importance must be placed on training on identification of red flags and suspicious patterns, reporting of suspicious transactions and timely engagement and cooperation with law enforcement agencies. In addition, strengthening AML/CTF controls and fostering a culture of compliance is key to safeguarding mobile payment service sector from fraud, ML/TF and other financial crimes.