SecurityGen
Telecom Security. Transcending Generations.

Understanding and Mitigating Mobile Money Fraud

In the era of digital finance, mobile money has emerged as a transformative tool, providing financial services to millions of people worldwide. However, alongside its immense benefits, mobile money platforms are increasingly becoming targets for fraudulent activities. Mobile money fraud, a multifaceted phenomenon, poses significant risks to service providers, customers, agents, and stakeholders alike. In this article, we delve into the intricacies of mobile money fraud, exploring its various forms, underlying causes, and potential mitigation strategies.

Mobile money fraud encompasses a spectrum of fraudulent activities occurring within the ecosystem of mobile money services. These activities target assets owned or managed by mobile money service providers, ranging from monetary assets to intangible assets such as brand reputation. Resulting in harm to the mobile money service provider, its customers, agents, or other parties. Understanding the diverse forms of mobile money fraud is crucial for implementing effective preventive measures.

Impersonation:

One prevalent form of mobile money fraud involves impersonation, where fraudsters deceive individuals to gain unauthorized access to their accounts or sensitive information. Techniques like **social engineering, SIM swap, and identity theft** are commonly employed to perpetrate impersonation fraud.

Insider Fraud:

Another significant threat arises from within the mobile money ecosystem itself. Insider fraud occurs when individuals within the organization abuse their access privileges for illicit purposes. This may include **corruption, data leakage,** or other forms of internal misconduct, jeopardizing the security and integrity of the mobile money service.

Agent Fraud:

Mobile money agents, vital intermediaries in the service delivery chain, are also susceptible to fraudulent activities. Agent fraud encompasses various schemes, such as manipulating **commissions, imposing illegal fees on** customers, or engaging in unauthorized **cash-in and cash-out transactions,** thereby compromising the trust and reliability of the entire system.

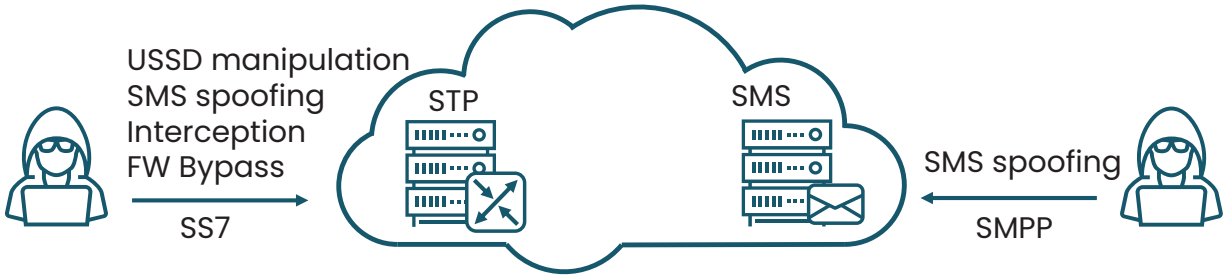
Cyber Fraud:

The rapid digitization of financial services has opened new avenues for cybercriminals to exploit vulnerabilities in mobile money platforms. Cyber fraud tactics range from **hacking into systems to intercepting data through man-in-the-middle attacks or spoofing legitimate entities,** posing significant challenges to the security infrastructure of mobile money services.

Given the evolving nature of mobile money fraud, it is imperative for stakeholders to proactively implement robust measures to detect, prevent, and mitigate fraudulent activities. To achieve this, continuous monitoring, data analytics, and collaboration among stakeholders are essential.

Mobile Money Fraud on Signaling Interfaces

The main threats of mobile money fraud of signaling interfaces are SMS spoofing, USSD manipulation, interception of OTP codes, and firewall bypass.



Fraud Risk Assessment program

SecurityGen introduces a fraud risk assessment program specifically aimed at testing scenarios that can lead to mobile money cyber fraud. It covers cases such as money transfer via SMS and USSD, the possibility of spoofing and intercepting SMS, manipulation with USSD commands, A2P fraud, and firewall bypass checks.The full list of test cases is presented in the table below.

SMS spoofing

SMPP interface:

- Money transfer via SMS commands
- MO/MT SMS spoofing check
- A2P SMS termination
- Partner impersonation check

SS7 interface:

- Money transfer via SMS commands
- MO/MT SMS spoofing check
- A2P SMS termination

USSD manipulation

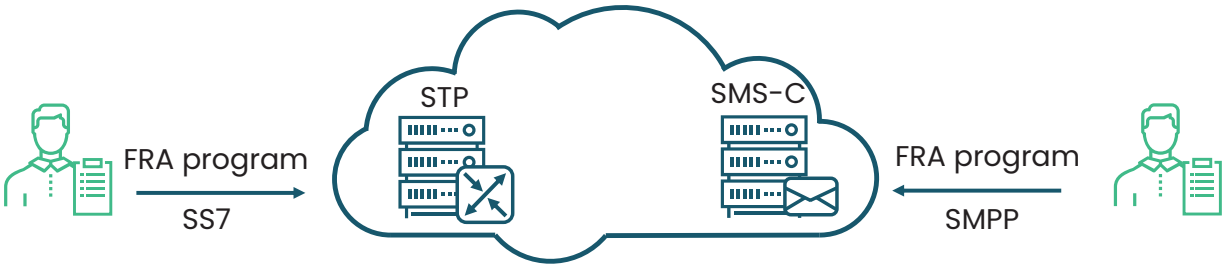
- Money transfer via USSD commands
- USSD manipulation check

Interception

- OTP SMS interception

Firewall bypass

- SS7 firewall bypass techniques
- SMS firewall bypass techniques



Fraud Risk Assessment Prerequisites

FRA on SS7 interface:

- Two test phones with positive balance
- Mobile Money services enabled
- Signed Authorization Letter
- No blacklisting of the tester GT

SMPP interface:

- Two connections via SMPP with a partner credentials
- Two test phones with positive balance
- Mobile Money services enabled
- Signed Authorization Letter

Fraud Risk Assessment Outcome

- Check the antifraud protection from an intruder point of view
- Find the network vulnerabilities that can lead to mobile money fraud execution
- Find general firewall bypass techniques
- Recommendations how to improve network protection against fraud

In conclusion, Mobile money fraud poses significant challenges to the integrity and security of financial ecosystems. By understanding the various forms of fraud, implementing robust preventive measures, and fostering collaboration among stakeholders, mobile money service providers can effectively mitigate the risks associated with fraudulent activities, ensuring the continued trust and viability of mobile money services in the digital age.