GSMA

March 2024

Mobile money fraud typologies and mitigation strategies

GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive.

Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com

GSMA Mobile Money

The GSMA's Mobile Money programme works to accelerate the development of the mobile money ecosystem for the underserved.

For more information, please contact us:

Web: www.gsma.com/mobilemoney
X: @GSMAMobileMoney
Email: mobilemoney@gsma.com

BILL & MELINDA GATES foundation

The Mobile Money programme is supported by the Bill & Melinda Gates Foundation.

Authors

Winnie Wambugu

Contributors

Kennedy Kipkemboi Sawe

Acknowledgements

Ashley Olson Onyango

Stealth Africa Consulting LLP

We extend our gratitude to MTN Mobile Money Uganda and M-Pesa Africa for their valuable contribution to the case studies.

Published March 2024

Contents

Contents

01

Abbreviations

Abbreviation	Description
ACFE	Association of Certified Fraud Examiners
AI	Artificial intelligence
API	Application programming interface
CICO	Cash-in cash-out
GSMA	Global System for Mobile Communications Association
MNO	Mobile network operator
MMSP	Mobile money service provider
MSISDN	Mobile station international subscriber directory number
SIM	Subscriber identity module
DFS	Digital financial services
CGAP	Consultative Group to Assist the Poor
COC	Code of conduct

02

Introduction

2.1 Background and importance of this study

Loss of funds to fraud in mobile money can lead to a loss of trust in digital financial services, undermining financial inclusion and global development goals. Mobile operators and financial service providers face liability and reputational losses when customers lose money, with loss of reputation being more difficult to recover. Service providers can maintain customer trust and adoption of mobile money by responding to fraud threats and regularly reviewing and updating their fraud controls – this requires investing in technology, resources, and training.[1]

Mobile money systems are essential to the transformation of inclusive financial interactions in a world that is rapidly digitising. While this transformation has had positive socio-economic outcomes, the growth of mobile money presents complex challenges. As global adoption of mobile money services increases, so do fraudulent schemes propagated through mobile money systems. The impact of mobile money fraud extends across various stakeholders. Users may experience financial losses, mental anguish, exposure of personal information, and may avoid using mobile money altogether. On the other hand, service providers face reputational damage and financial liabilities. Although mobile money service providers have been criticised for not taking enough proactive anti-fraud measures, it's evident that they have taken steps to protect their customers. Nonetheless, the industry still faces a key challenge in anticipating how fraudsters may exploit the technology involved in mobile money systems.

The inherently digital nature of mobile money systems, while enhancing accessibility, is vulnerable to a range of fraudulent activities consistent across different markets. These include intricate technical breaches and subtle social manipulation to plan attacks that circumvent current fraud prevention measures. A comprehensive understanding of these threats is vital to ensuring the stability of financial processes for both users and providers.

As the financial sector becomes more digitalised, more stakeholders - including the authorities - have raised concerns. Regulators seek to find balance between fostering innovation and protecting end users. Despite the growing awareness of mobile money fraud, there is a gap in comprehensive research encompassing fraud typologies, trends, patterns, and effective mitigation strategies. This paper attempts to address this gap by providing an analysis of several fraudulent schemes widespread in mobile money platforms, as well as common prevention and mitigation techniques.
This study aims to provide stakeholders with the knowledge required to understand and navigate mobile money fraud challenges, foster secure environments, and ensure the sustained growth of mobile money as a transformative financial tool.

As global adoption of mobile money services increases, so do fraudulent schemes propagated through mobile money systems.

1 GSMA. (2020, March). Mitigating Common Fraud Risks: Best Practices for the Mobile Money Industry. Saad Farooq (Ed.).

2.2 Research objectives and scope

The purpose of this study is to assess and classify the various forms of fraud that can occur in mobile money systems and to identify general tendencies and strategies typically employed by mobile money fraudsters. The study also intends to propose useful tactics, tools, and guidelines for preventing, detecting, and responding to occurrences of mobile money fraud. The scope and objectives of the study are outlined as follows:

Examine, identify, and categorise the different types of fraudulent activities within mobile money systems, including - but not limited to - social engineering, technical exploitation, identity fraud and other common schemes.

Analyse the trends and patterns in mobile money fraud, including the most common methods fraudsters use, the frequency of fraud incidents and the regions most affected by social engineering, technical exploitation, identity fraud and other common schemes.

Recommend effective strategies and tools to prevent and combat mobile money fraud, including regulatory measures, fraud prevention technologies, and consumer education programs.

Provide a comprehensive overview of the fraud landscape in mobile money, including common fraud schemes and techniques used by fraudsters, social engineering, technical exploitation, identity fraud and other common schemes.

Provide guidance to mobile network operators, regulators, law enforcement agencies and other stakeholders on effectively preventing, detecting, and responding to mobile money fraud incidents.

03

Executive summary

3.1 Fraud typologies

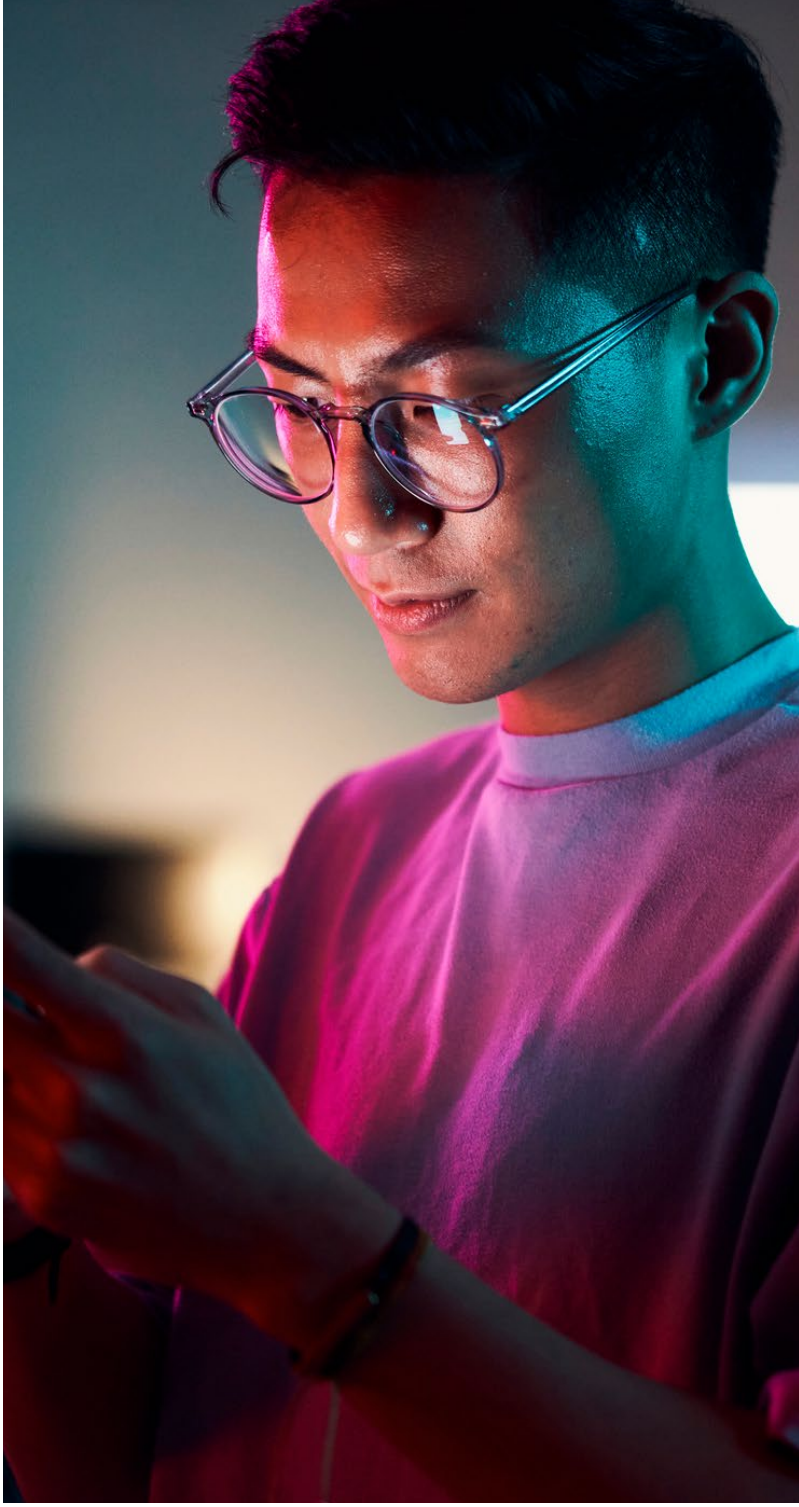
Fraudulent activities prevalent in mobile money can take on several forms, utilising both traditional and advanced technical methods. Gaps in terms of mobile money fraud typologies framework and classification could impede efforts to address fraud mitigation strategies collectively and globally.

This report explains the intricacies of mobile money fraud typology and defines the various types of mobile money fraud. Our research shows that a blended form of categorisation could help ensure that all mobile money fraud schemes and sub-schemes are identified, defined and ultimately addressed. We classify the main categories as *impersonation, insider fraud, agent fraud,* and *cyber fraud.*

Fraud schemes that fall under these broad categories discussed in this report include:

1. social engineering
2. identity fraud
3. SIM swap and account takeover fraud embezzlement
4. data theft and system breach
5. corruption
6. agent commissions fraud
7. cash-in-cash-out fraud
8. illegal fees and services
9. confidentiality breaches
10. KYC breaches
11. malware and hacking schemes
12. man-in-the-middle attacks
13. denial-of-service (DoS)
14. phishing
15. spoofing

This report further outlines interconnection between the fraud categories discussed providing valuable insights into how different types of mobile money fraud often coalesce and collaborate, creating a more comprehensive understanding of the complex dynamics at play within the mobile money ecosystem.



Our research shows that a blended form of categorisation could help ensure that all mobile money fraud schemes and sub-schemes are identified, defined and ultimately addressed.

3.2 Trends and patterns in mobile money fraud

Our research covered a comprehensive scope involving 34 countries in Africa, Asia, and Latin America, participating through consultations, interviews, and survey. Our survey focused on professionals within the mobile money ecosystem, particularly those with extensive knowledge of - and experience in – mobile money fraud, with 76% of respondents in middle to senior management roles.

Our survey focused on the dynamics of various fraud schemes, and identified impersonation schemes as the most prevalent. Identity fraud ranked as the highest mobile money fraud scheme at 90.38%, followed by social engineering schemes at 88.46%, and another impersonation scheme, SIM swap fraud, ranking fourth at 78.85%. Insider fraud ranked third at 86.54% and cyber fraud ranked fifth at 59.62%.

Insider fraud and threats emerged as a significant concern among respondents, with 94% expressing concern about insider fraud perpetrated both by those inside and outside the relevant organisation. Notably, collusion with external fraudsters to commit fraud was identified as the top insider fraud scheme at 88.24%. Internal actors include not only staff of a mobile money provider, but also insiders in agents and third parties - 22% of respondents indicated that fraud often involved third-party service provider staff, such as IT integrators.

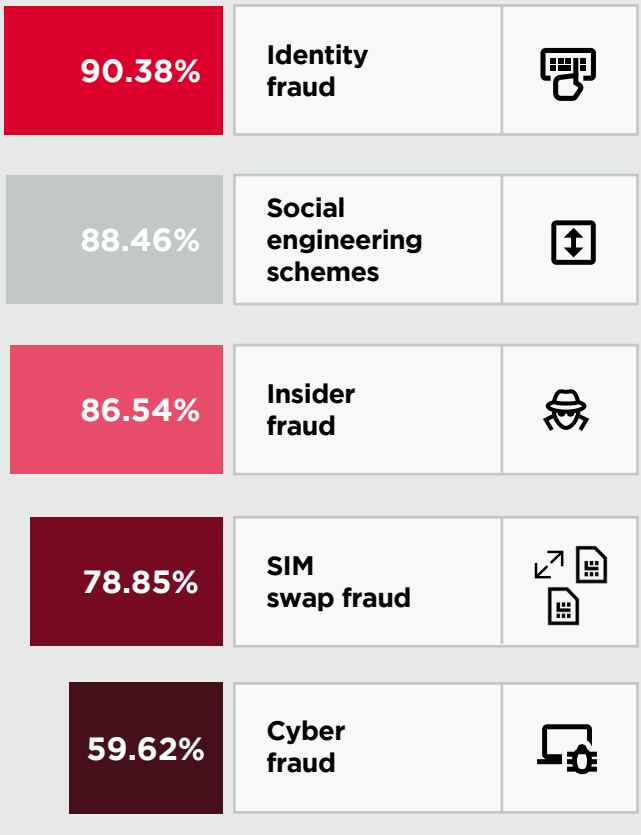
This study demonstrates the efforts to manage fraud by mobile money providers. Many of them have a formal taxonomy, implemented fraud management systems, put in place anti-fraud controls, executed successful awareness campaigns, and implemented customer recourse and reporting channels. A vast majority, 96.08%, report mobile money fraud cases to authorities. However, they also recognise that mobile money fraud is increasing, with 84% respondents indicating as such. Some of the post-covid factors have been identified as contributors to the increase in mobile money fraud including the surge in mobile and online transactions (88.24%), the shift to remote work arrangements (72.55%), and pandemic-related technology changes (64.71%).

While 94.12% indicated that they have fraud management systems in place, 54.90% raised concerns about the effectiveness of these systems, with only about 10% using advanced technologies such as artificial intelligence (AI) and machine learning to address the issue. We found that formal fraud risk assessments were not conducted by 49.02% of respondents, potentially leaving organisations vulnerable to unforeseen risks. Our study found that general anti-fraud controls are largely in place, suggesting that mobile money providers are making purposeful efforts to combat fraud and have invested in areas such as awareness and training, detection and monitoring systems, dedicated fraud teams and board oversight to manage fraud better.

Our study found that 96% of providers detected mobile money fraud through customer complaints, emphasising the crucial role of customer awareness and reporting channels. Regulators were deemed moderately supportive in the fight against mobile money fraud. However, a majority of respondents, 70.59%, found law enforcement authorities to be ineffective, citing reasons such as a lack of technical capacity, poor resourcing, and corruption as key factors contributing to this ineffectiveness.

The survey provides comprehensive insight into the state of mobile money fraud, demonstrating both strengths and areas requiring attention within the industry. The results underscore the need for a more sophisticated, multi-layered approach to managing mobile money fraud, involving technological advancement, cross-sector collaboration, and continuous adaptation to the evolving landscape of mobile money fraud.

Figure 1



04

Understanding mobile money fraud typology

4.1 Definition of mobile money fraud

The Association of Certified Fraud Examiners (ACFE), the world's leading anti-fraud body, defines fraud as any activity that relies on deception in order to achieve a gain. Fraud becomes a crime when it is a "knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment".[2] A mobile money service entails money transfers, as well as making and receiving payments via a mobile device. The following are the benchmarks of a mobile money service as defined by GSMA:[3]

- The service must offer a network of physical transactional points which can include agents, outside of bank branches and ATMs, that make the service widely accessible to everyone. The agent network must be larger than the service's formal outlets.
- The service must be available to the unbanked, for example, people who do not have access to a formal account at a financial institution.
- Mobile banking or payment services (such as Apple Pay and Google Pay) that offer the mobile phone as just another channel to access a traditional banking product are not included.

Mobile money fraud can therefore be defined as fraud that takes place on assets owned or held by a mobile money service to the detriment of a mobile money service provider, its customers, agents or third parties. Assets include money, information, and intangible assets such as brand, reputation, or services.

2 Association of Certified Fraud Examiners (ACFE). (2023). https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud
3 Raithatha, R., et al. (2023). The State of The Industry Report on Mobile Money. GSMA.

4.2 Why mobile money is unique from a fraud perspective

Mobile money fraud is unique for the following reasons:

- **Victim profile:** The service is available to the unbanked and underbanked who live precarious financial lives with many having low literacy levels. These customers are therefore vulnerable to deception techniques such as social engineering schemes. As one of our interviewees from Pakistan revealed, customers sometimes hand over their mobile phones to agents to assist them perform transactions due to low literacy levels.

- **Availability:** The services are ubiquitous and available 24/7. The potential victim population is therefore wide, and fraud can happen at any time.

- **Velocity of funds:** The settlement process in most cases is instant and may not go through a clearing process. Once a transaction is initiated and confirmed by a customer, it is instantly completed. This is different from, for instance, bank transactions, that go through a settlement and clearing process.

- **Randomness of target victims:** A fraudster does not necessarily need to know a target victim since a mobile number can be randomly guessed due to sequential numbering of mobile numbers – MSISDNs (mobile station international subscriber directory numbers). This is different from, for instance, a bank account number that is not easy to randomly determine.

- **Distance between victims and perpetrators:** Most transactions happen remotely without any face-to-face interaction among parties. This makes it possible for fraudsters to target victims without being identified physically or by eye, and from a different geographical location.

- **Complexity of ecosystem:** The mobile money ecosystem is complex with many players such as mobile money service providers, agents, technology service providers, integrators, financial institutions and intermediaries, merchants, retailers, utility companies and government entities some of which are customers and regulators. These have multiple interlinked channels that provide convenience to customers. However, this also provides several exfiltration points for stolen funds. For instance, money stolen from a bank account can be withdrawn from an agent network through money mules. In this case, this is not mobile money fraud, but banking fraud using the mobile money network as a conduit.

- **Multi-stage fraud schemes**: Mobile money fraud can involve several types of schemes before it is ultimately executed. For instance, a social engineering scheme can be used to obtain information to commit a SIM swap fraud leading to account takeover and identity theft so that a banking fraud is committed through impersonation. This makes fraud classification challenging as social engineering, SIM swap fraud, identity fraud and banking fraud are all fraud categories. We explain these schemes in subsequent sections of this report.

- **Losses per victim:** The fraud losses are on average relatively small compared to other fraud claims witnessed in mainstream banking, for instance. While this may constitute significant loss on the part of the consumer, they may not be viewed as such by law enforcement officers. In addition, few victims will follow up on fraud cases to a logical conclusion.

- **A fast-evolving service:** Mobile money services are quickly evolving with new innovations to improve quality of service and to transform lives. New integrations to other services are taking place frequently through APIs as technology evolves. Services are also fairly new compared to formal banking services that have mature processes. Fraudsters are always up-to-date with these changes - however, many customers are not, leading some to fall victim to fraud.

For these reasons, mobile money fraud has a unique typology compared to those of traditional fraud such as those detailed in the ACFE Fraud Tree. It requires a deeper appreciation of its complexities, a greater understanding of its connections to other forms of fraud (which are at times misclassified as mobile money fraud), and a comprehensive and collaborative approach to deal with them.

4 Association of Certified Fraud Examiners (ACFE). (2023). https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud

4.3 Forms of classification of mobile money fraud

85.71% of our survey respondents indicated they had formal, established categories for mobile money fraud in their organisation, with 92.86% indicating that a standardised fraud classification is useful for mobile money fraud. As it stands, there is no consistent uniform framework for classifying typologies. However, some studies have investigated these typologies, providing nuanced perspectives on the multifaceted aspects of mobile money fraud. Defined categories are determined by the specific contextual considerations of the respective analyses or studies. Classifications in this section are derived from a variety of sources - specific fraud schemes are as follows:

4.3.1 Attack vector categorisation

IT/cyber fraud: This involves leveraging vulnerabilities in technological systems, software, or hardware components, networks, or internet to gain unauthorised access to commit fraud. In the context of mobile money fraud, this category includes attack vectors that exploit technical weaknesses such as software vulnerabilities, insecure network connections, and unauthorised access to devices. Subcategories include hacking, man-in-the-middle attacks, denial-of-service (DOS), malware (trojans, spyware, viruses, worms, bots and ransomware), phishing, and spoofing. Although malware is used by hackers, not all malware is used for hacking, hence the need to classify it separately.

Impersonation: This refers to the act of pretending to be another for the purpose of deceiving them. In the context of mobile money fraud, this category includes attack vectors such as social engineering, identity fraud, and SIM swap or account takeover fraud. This research demonstrates that SIM swap fraud is a form of impersonation, since one takes over a mobile number and/or wallet of another for the purpose of accessing customer funds or to impersonate the customer for another fraud scheme.

Process-driven fraud: This refers to exploiting weaknesses or gaps in products, procedures and workflows to commit fraud. In the context of mobile money fraud, this category encompasses attack vectors that manipulate or circumvent processes and protocols, often by taking advantage of gaps, misconfigurations, miscommunication, lack of oversight, or non-adherence to procedures. For instance, agent commission/ arbitrage fraud would fall under this category since the agent exploits commission tariff loopholes to earn more commission by generating transactions that are not genuine.

Classification with these methods means clearly understanding the attack vector. For instance, a hacker can enter a system by exploiting system vulnerabilities to steal customer funds. The attack vector in this case is the system pathway, and therefore the fraud would be classified as cyber fraud. If the fraudster used social engineering schemes to steal the same customer funds, the categorisation would be impersonation. Although both cases feature stolen funds, the method determines the category, not the ultimate act of fraud, which is asset misappropriation of customer funds. The main advantage of using attack vector-based methodology is that it can be useful in identifying the weaknesses, loopholes and vulnerabilities that have been exploited. An attack vector can also affect various groups across the service, for instance impersonation schemes can affect staff, customers, agents and third parties.

85.71% of our survey respondents indicated they had formal, established categories for mobile money fraud in their organisation, with 92.86% indicating that a standardised fraud classification is useful for mobile money fraud.

4.3.2 Sector or group categorisation

This is a form of categorisation by a segment or group in the mobile money ecosystem identified by their shared characteristics. The main players in mobile money are the service provider(s), customers, and the distribution network. The following are the main categories:

Consumer/customer fraud: This type of fraud directly targets mobile money service consumers. 88.1% of our survey respondents indicated that consumers are the most severely impacted group by mobile money fraud. The purpose of this category is to emphasise how fraud directly impacts the consumer. However, the challenge is that most fraud types affect consumers, and this results in generalising during categorisation.

Insider fraud and treat: This involves employees within the mobile money ecosystem who exploit their position for illegal gains. It is a type of fraud or threat that comes from the inside – a current or former employee, contractor, or business partner that can carry out a fraudulent scheme by taking advantage of knowledge, skill, experience, or gain access with inside knowledge.

Agent (distribution network) fraud: This is fraud on or by agents. The fraud schemes under this category include commission/arbitrage fraud, CICO fraud, counterfeit currency schemes, and illegal fees and charges.

The main aim of this form of categorisation is to give attention to the segments and develop mitigation strategies aligned to each one. For instance, most customer fraud is through impersonation schemes which could be addressed by sustained awareness programs targeting customers - as we will demonstrate in one of our case studies. At the same time, much agent fraud can be addressed through agent monitoring (both system and physical monitoring through mystery shopper exercises) and enforcement measures.

4.3.3 Other forms of categorisation

The following are other less prominent forms of categorisation:

Degree of sophistication: This form of classification considers complexity of the fraud as follows:

- Low-tech/basic fraud: Simple and basic fraud methods that do not require advanced technical skills such as impersonation schemes where a customer is deceived into providing information or transferring money.
- High-tech/advanced fraud: Sophisticated fraud techniques that use advanced technology, multiple schemes, players and/or expertise to execute fraud. For instance, cyber fraud involving insiders and infiltration of multiple platforms.

Mobile service deployment lifecycle:[5] This classification is based on the stage of the mobile money deployment. Some categories include customer acquisition stage, transaction activation stage, and value addition stage.

Victim profile: This classification is based on the targeted victim such as:

- Individual-targeted fraud: Fraud directed at individuals or end users, for example customers through social engineering schemes.
- Business-targeted fraud: Fraud targeting businesses, merchants, or service providers in the mobile money ecosystem, for example a business-to-customer (B2C) payment solution targeted through hacking.

Our research found that the different forms of classification provide insights into how fraud can be categorised and that there is no 'one size fits all' solution. Instead, a blended form of categorisation is more likely to help identify, define, and ultimately address mobile money fraud schemes and sub-schemes.

4.4 Mobile money fraud typology and fraud schemes

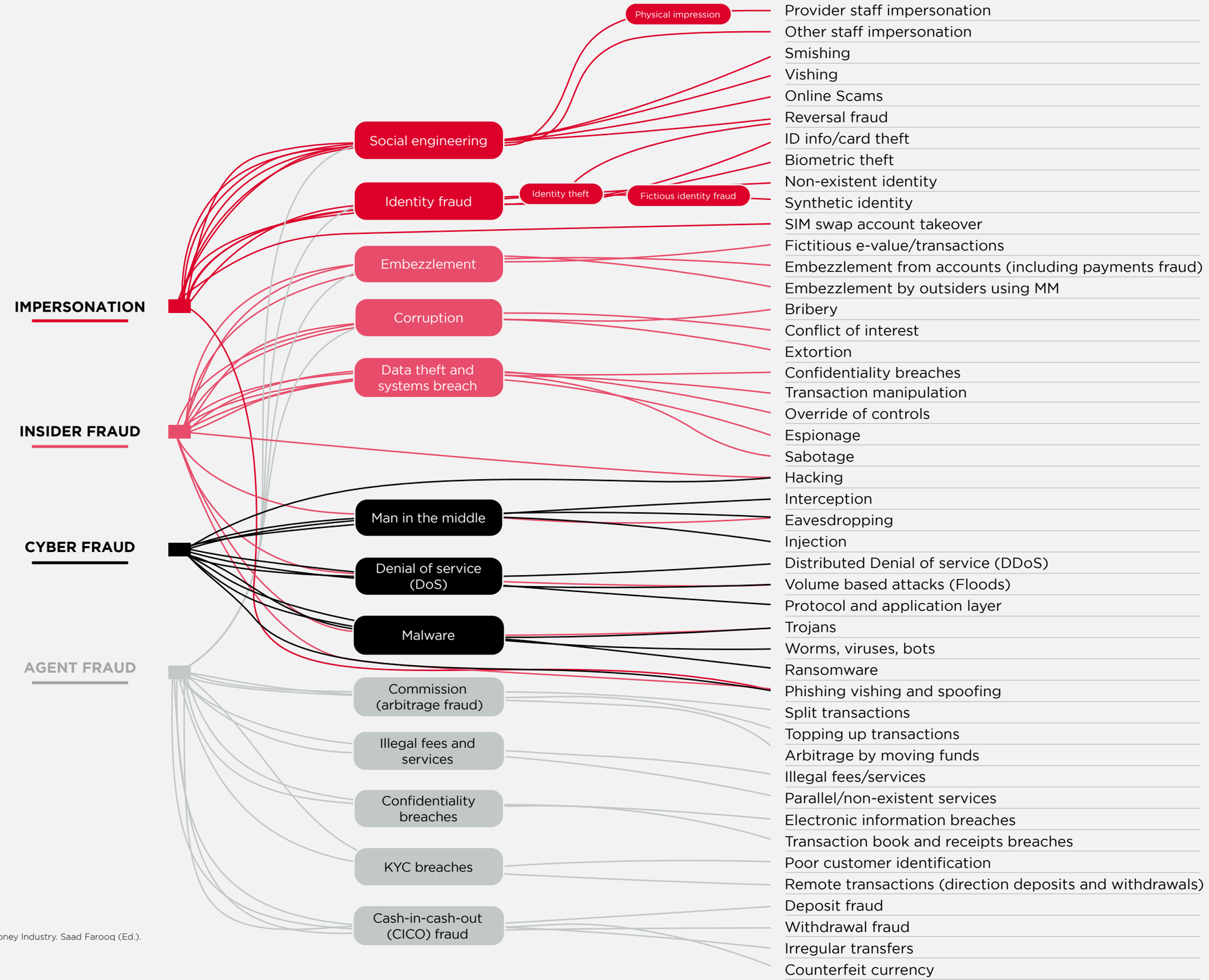
The paper 'Mitigating Common Fraud Risks: Best practices for the mobile money industry' discusses the most common and impactful forms of fraud within the mobile money industry. Some fraud types mentioned include account takeover fraud, social engineering fraud, identity fraud and malware attacks.[6]

Other studies show that fraudsters may use a combination of techniques to carry out more sophisticated fraud schemes, such as SIM swap fraud, where fraudsters take control of a user's mobile phone number to gain access to their mobile money account.[7]

During our review of these fraud schemes and types, we found that a blended classification approach gives prominence to the key mobile money fraud schemes by both sector and by attack vector. This is because focusing on only one instead fails to recognise others of equal importance. For instance, as our research shows, mobile money practitioners find both impersonation schemes and insider fraud as the highest mobile money fraud schemes, although their classification is different.

We have therefore classified the main categories as **impersonation**, **insider fraud**, **cyber fraud** and **agent fraud**. The diagram below illustrates the taxonomy of mobile money fraud and interconnection between fraud schemes:

Figure 2: Mobile money fraud taxonomy



5 Mudiri, J. L. (n.d.). Fraud in Mobile Financial Services. Hyderabad: MicroSave.
6 GSMA. (2020, March). Mitigating Common Fraud Risks: Best Practices for the Mobile Money Industry. Saad Farooq (Ed.).
7 Raithatha, R., et al. (2023). The State of The Industry Report on Mobile Money. GSMA.

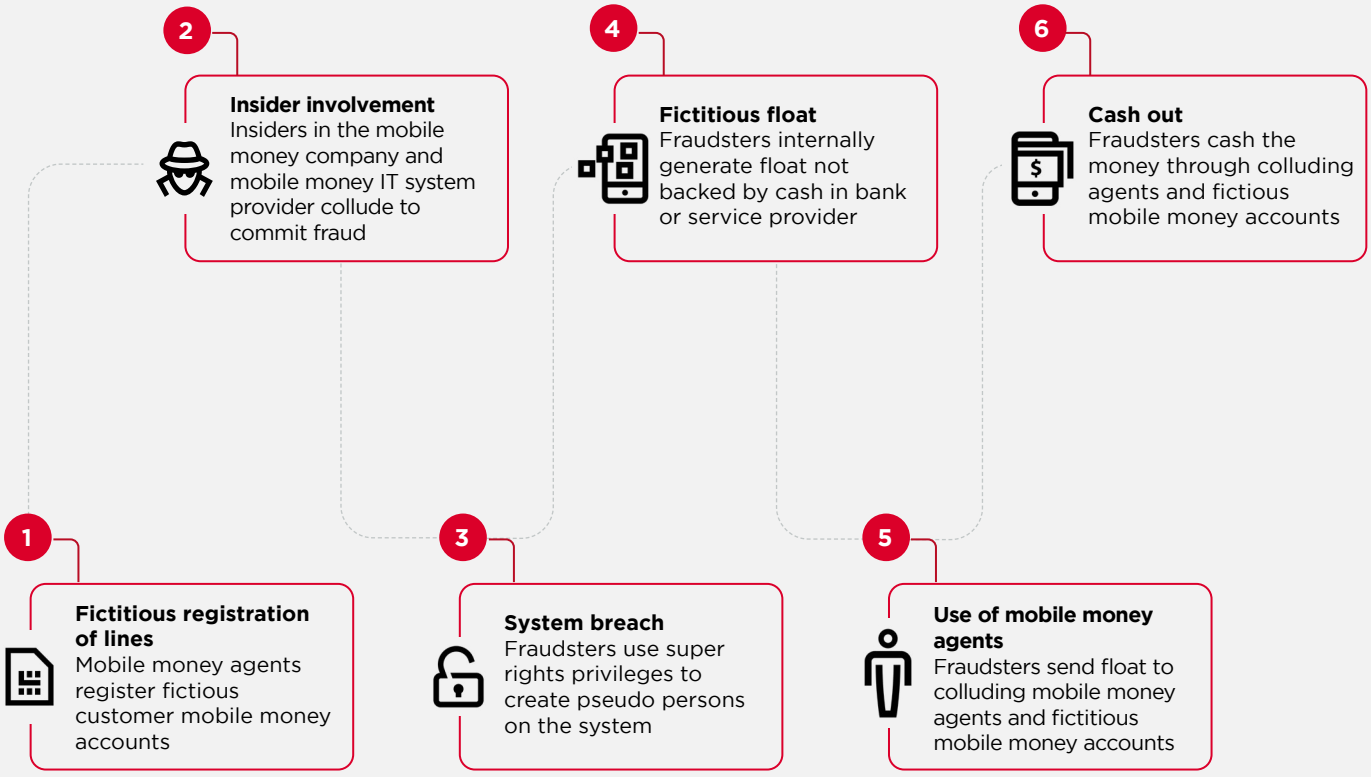
Case study

Fraud with multiple fraud schemes

In mobile money it is common for fraud to involve several types of schemes before they are ultimately executed - we term these 'multi-stage schemes'. This case study focuses on the connections between fraud categories, and how these provide valuable insights into how the various types of mobile money fraud often coalesce. The objective is to understand how to create a more comprehensive understanding of the complex dynamics at play within the mobile money ecosystem.

In this scenario, insiders at a mobile money company and IT mobile money system provider collude to steal money from the mobile money system. They do so by creating fictitious journals and by transferring money through agents and fictitious customer mobile money accounts created for the sole purpose of receiving and withdrawing the funds. The fraudsters abuse super-user rights and create pseudo persons on the system who transact as a 'ghost' person and internally generate, float or create e-money on the mobile money system. They then transfer the e-money to agents and fictitious customer mobile money accounts before cashing the money out. The fraud is carried out by exploiting weaknesses such as lack of reconciliations, maker-checker approval processes, user rights management in creating e-value, agent transaction monitoring, and failure in customer limit controls. This scheme is illustrated in the diagram below:

Figure 3: A journey of fraud with multiple schemes



How to determine classification

The simplest way to determine this fraud scheme is by identifying the primary driver, vector or element in the mode of execution. In most cases, one aspect is more dominant, for instance, if insiders were the main executors of fraud, as is the case in the case study above, then it can be primarily categorised as insider fraud. We will now proceed to define these categories and the various fraud schemes and scenarios they apply to.

4.4.1 Impersonation

This refers to 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. In the context of mobile money fraud, this category includes:

Social engineering:
This involves an act of pretending to be another to manipulate someone into divulging information, granting unauthorised access, or performing certain actions leading to fraud. This type of fraud involves impersonation and deception. Fraudsters can pretend to be mobile money staff, agents or staff of other organisations. The subcategories are:

Physical impersonation:
This is social engineering through physical interaction between a fraudster and the victim. For example, a physical impersonation of provider staff would be imposters pretending to be provider staff at an agent outlet. They ask to 'inspect' agent activities. They take copies of customer transaction information and save their number on the agent's phone in the name of a mobile money provider while distracting agent staff at the outlet. They later call the agent with saved contact and customers using details obtained in the transaction book and trick them to transfer funds or to provide personal details that enable fraudsters to carry out SIM swaps. They then transfer funds from the agent and customer accounts.

Smishing – text messaging:
This involves sending messages via SMS or other mediums to deceive another into sending money. An example is when fraudsters send messages of fake winnings of a provider promotion. They ask the customer to pay a processing fee.

Vishing – phone calls:
This involves a fraudster calling and impersonating a mobile money provider staff or others to deceive another to divulge information or perform certain action leading to fraud. An example is where a fraudster calls pretending to be mobile money provider staff. The customer is tricked into entering 'codes' to upgrade their MSISDN details. The customer follows prompts and unwittingly transfers money from their mobile money wallet.

Online scams:
Scams occur through online platforms such as social media and deceive others into sending money. This includes impersonation of organisations such as utility service providers to receive payments through business and merchant accounts that have been fraudulently registered. For example, fraudsters put up fake advertisements involving the sale of fictitious property or merchandise and trick customers into sending money. The fraudster's mobile money accounts that receive funds have fake identities, making recovery, arrests, and prosecution difficult.

Reversal fraud:
his is a deceptive practice where a consumer intentionally initiates a payment reversal or chargeback for a legitimate mobile transaction they've made, with the intention of receiving a refund while retaining the purchased goods or services. In payment reversal fraud, the fraudster takes advantage of consumer protection mechanisms provided by the mobile service provider.

> Please note that phishing and spoofing are also types of social engineering schemes. However, for purposes of mobile money fraud, we have classified them under cyber fraud as the attack vector is IT-related.

Identity fraud:
This is a form of impersonation that involves taking over a genuine identity of another or creating a fictitious, non-existent identity. This has two subcategories: identity theft and fictitious identity fraud. Identity fraud is mostly carried out at the point of subscription:

Identity theft:
Theft of someone's personal information to commit fraud. Perpetrators usually obtain personal information or documents such as identity (ID) numbers or cards, biometrics or passwords and use them to assume the identity of others. In the context of mobile money, the subcategories are ID card or information, and biometrics.

- **ID card or information:** This is the use of genuine stolen identity cards, or information in identity cards, to register fake mobile money accounts. For example, scammers obtain ID cards that are lost or stolen. They register mobile money accounts using identities. They then borrow money from lending platforms. After receiving funds through mobile money, they dump the MSISDNs. Customers later get contacted by a credit recovery agency to pay back money they did not borrow. In some instances, customers are blacklisted by a credit reference bureau before the matter is settled.

- **ID card or information:**
  This is the use of genuine stolen identity cards, or information in identity cards, to register fake mobile money accounts. For example, scammers obtain ID cards that are lost or stolen. They register mobile money accounts using identities. They then borrow money from lending platforms. After receiving funds through mobile money, they dump the MSISDNs . Customers later get contacted by a credit recovery agency to pay back money they did not borrow. In some instances, customers are blacklisted by a credit reference bureau before the matter is settled.
- **Biometrics:**
  This is the theft of biometric identity at the point of registration, transmission, or storage. This can also involve theft of copies of fingerprints or high-resolution pictures to access customer accounts.[8] For example, a mobile money agent initiating a subscription using a customer's biometrics pretends the registration fails, but in reality it was completed. The agent asks the customer to repeat the process again several times with different MSISDNs. The additional MSISDNs with customer biometrics are then used for a fraudulent activity.

Fictitious identity fraud:
This is the creation of non-existent, fictitious, or forged identities. The subcategories are:

- **Fictitious/non-existent ID:** This is the creation of a fake or non-existent identity. Technically, this is not identity theft since the identity is not stolen but created. An example is when fraudsters create forged identity cards or details and register mobile money wallets. Before a mobile money provider verifies the identity in a validation process, fraudsters use these MSISDNs for a fraudulent activity. Such MSISDNs are mostly used for quick exfiltration funds in other scams.

- **Synthetic identity theft:** Synthetic ID fraud occurs when new identities are made by blending elements from multiple individuals. Synthetic fraud can simultaneously affect several customers, but make it difficult to identify who has been impacted. An example is when a fraudster obtains genuine ID numbers then uses photos obtained from social media to create a new identity. If a MSISDN is for instance validated using ID number and details which are genuine, then registration may be successful. The fraudster then uses the MSISDN for a fraudulent activity making recovery, arrests, and prosecution difficult.

SIM swap and account takeover fraud:
These are forms of impersonation as one takes the identity of another by taking over their SIM card and/or mobile money account or wallet. SIM swap is distinct from account takeover since a SIM swap can be used to take over a mobile number to carry out another fraud scheme - for instance, to impersonate a customer in a call to validate a fraudulent transaction.

It should be noted that SIM swap is considered a form of identity theft.[10] However, it is separate from identity theft insofar as SIM swap fraud has a unique attack vector and its mitigation strategies may be different from other forms of identity theft in the context of mobile money.

SIM swap fraud:
This occurs when a fraudster tricks a provider into porting or transferring a victim's phone number to a new SIM card under the fraudster's control. The subcategories are:

- **SIM swap for account takeover:** The fraudster gains access to the victim's mobile number and/or wallet or account. For example, a scammer calls or sends a message to a mobile money user pretending to be a customer support agent and convinces the customer to reveal their personal identification number (PIN) or other details such as ID number under the guise of fixing a technical issue. The victim shares details and the SIM card is swapped. The customers mobile money account is then accessed and funds withdrawn at an agent outlet or transferred to another account.

- **SIM swap for another fraud scheme:** The perpetrator takes over the SIM/MSISDN to impersonate the subscriber to commit another fraud scheme. For example, a fraudster obtains the PIN number and other details such as ID number, date of birth and recent transactions and uses them to swap the MSISDN. The fraudster then targets customer bank account(s) with transfers to other bank or mobile money accounts. The bank calls the swapped MSISDN to confirm if the transactions are genuine. The fraudster, now purporting to be customer, confirms them. The transactions are cleared and the funds are stolen.

8 Chalwe Mulenga, M., Duflos, E., & Coetzee, G. (2022). The Evolution of the Nature and Scale of DFS Consumer Risks: A Review of Evidence CGAP.
9 Ibid

When inside the account, the fraudster can make unauthorised transactions, transfer funds to other accounts, or even withdraw money through mobile money agents.

Account takeover fraud:
This is the unauthorised access and control over a legitimate mobile money user's account/wallet. This may involve exploiting vulnerabilities in the account security measures, such as weak passwords, poor authentication procedures, or social engineering tactics, to gain unauthorised access to the account. An example is when acquired account information is used to attempt to bypass security measures, this may include PINs, passwords, and security questions to access the victim's account. When inside the account, the fraudster can make unauthorised transactions, transfer funds to other accounts (including their own), or even withdraw money through mobile money agents. In some cases, the fraudster might attempt to change the account settings, such as contact information, to hinder the victim's ability to regain control and receive notifications about the fraudulent activity.

Please note that while SIM swap fraud can lead to account takeover, account takeover may also happen in other ways such as **account cloning**, where fraudsters create duplicate accounts using stolen information to mirror legitimate users' mobile money accounts and conduct fraudulent transactions.

Impersonation in other fraud categories

In **cyber fraud**, **phishing** emails often involve impersonation, where the attacker pretends to be a trustworthy entity, such as a bank, government agency, or well-known organisation.

Spear phishing targets specific individuals and often involves impersonating someone the target knows. Attackers may spoof email addresses to make it appear as though the email is coming from a legitimate source.

By impersonating a known or trusted sender, attackers aim to deceive recipients into believing that the communication is genuine, increasing the likelihood of success in the phishing attack. SIM swaps and account takeover can involve information acquired through hacking of a customer database and using personal information to carry out SIM swaps and takeover customer accounts.

In **agent fraud**, agents can carry out impersonation schemes because they are a key customer touchpoint at the lowest level in the ecosystem and have built trust in local communities. They can therefore deceive a customer to disclose their PIN, or engage in 'shoulder-surfing' a customer to see their PIN and other information in preparation for a SIM swap and account takeover. Shoulder-surfing is a type of social engineering technique used to obtain information such as PINs, passwords and other confidential data by looking over the victim's shoulder. Some providers allow agents to carry out SIM registration – as a result, they can also carry out identity fraud and theft, such as registering fictitious mobile money accounts.

[10] Safaricom. (2023). Sim swap fraud. https://www.safaricom.co.ke/fraud-awareness/impersonation/sim-swap-fraud

4.4.2 Insider fraud

This involves employees within the mobile money system who exploit their position for illegal gains or act to the detriment of others. This is a type of fraud or threat that comes from the inside – a current or former employee, contractor, or business partner that can carry out a fraudulent scheme by taking advantage of knowledge, skill, experience, or access as an insider.

86.55% of our survey respondents indicated that insider fraud is one of the leading fraud schemes in mobile money. For this reason, it is prevalent and needs unique focus in an organisation. In the truest sense, it is not a fraud scheme since an insider can potentially carry out any of the other fraud schemes as a result. However, insiders are a unique group or class in the mobile money ecosystem and can therefore perpetrate certain fraud schemes that others may not. For instance, corruption is a fraud scheme that is perpetrated by insiders. Insiders in the mobile money ecosystem exist among various players, as follows:

Mobile money service provider:
This is an employee who works in a mobile money service provider company with certain authority, knowledge, skill, and experience. These include back-office operations staff, agent network managers, sales staff, and trade representatives who visit agents regularly.

IT vendors and system integrators:
These are service providers whose staff have privileged system rights to various platforms that are integrated to the core mobile money system.

Merchants, payment service providers (PSPs) and other businesses (B2B and B2C customers):
These are businesses that rely on mobile money services to serve their customers. These include merchants, PSPs and financial institutions.

Mobile money agent:
These are agent staff such as agent assistants who interface with the customer at an outlet, or staff who work at the organisation's head office. They have access to agent tills, e-money/floats, cash, customer information in transaction books, and privileged system rights to agent network platforms.

In the context of mobile money fraud, this category includes:

Embezzlement:
Embezzlement is theft or misappropriation of funds placed in one's trust or belonging to one's employer. It often involves a trusted individual taking advantage of their position to steal funds or assets, most commonly over a period of time. Embezzlement can be carried out by a lone insider, in collusion with other insiders or with external fraudsters. The following are subcategories and examples of fraud schemes under embezzlement:

- **Fictitious e-value and transactions:** This is a scheme involving crediting float or e-value that is not backed up by cash deposited in bank escrow accounts. The float is then transferred to agents or mobile money accounts. For example, staff of a mobile money service provider creates fictitious float or e-value not backed up by cash deposits or funds transfers to providers bank account. The funds are cashed out using various agents. This happens due to poor user-rights management in creation of e-value and lack of proper reconciliations, among other reasons.

- **Embezzlement from accounts (including payments fraud):** This is theft from customers, agents (whether master, super-agent, or agent assistant of accounts or tills), merchant accounts, or cash collection accounts. For example, staff stealing funds from dormant mobile money wallets, since they know there's little chance of customer complaint. The perpetrator transfers the money to fictitious mobile money accounts registered for this purpose before withdrawing the funds. Another example is payment fraud, where insiders target B2B or B2C mobile money accounts by obtaining credentials, logging and transferring the funds to mobile money wallets.

- **Embezzlement with mobile money as a conduit to exit funds:** This is internal fraud which uses the mobile money platform as an exit or exfiltration route.

Corruption:
Corruption is defined by Transparency International as abuse of entrusted power for private gain,[11] meaning that it can only be perpetrated by those in a position of power. The following are subcategories and examples of fraud schemes under corruption:

- **Bribery:** This involves offering, giving, receiving, or soliciting something of value (often money) to influence the actions or decisions of an individual in a position of trust or authority. An insider can receive bribes or kickbacks to compromise systems or circumvent processes in mobile money. For example, a mobile money provider's employee accepts a bribe from a mobile money agent to prioritise their request and transactions over others or to ignore certain compliance checks.

11 Transparency International. (2023. What Is Corruption? https://www.transparency.org/en/what-is-corruption

- **Conflicts of interest:** This is a situation where an individual's personal interests, financial or otherwise, could compromise their ability to make impartial decisions or act in the best interests of an organisation, often leading to decisions that benefit them personally. For example, employees of a mobile money provider influence decisions that benefit a mobile money agent they have a personal financial interest in without disclosing this conflict of interest. This ultimately benefits the employee financially, giving one agent an unfair advantage over others and sometimes flouting established processes.

- **Extortion:** This is the act of coercing or threatening someone to do something against their will, often involving the threat of revealing damaging or sensitive information, with the intention of gaining money, property, or some other advantage. For example, staff threaten to sanction or punish an agent on fake or flimsy grounds unless they pay money to them or colluding agents, and threatening to deny services unless they pay the bribe.

Data theft and system breach:
This is one of the major forms of insider threat. Data theft refers to the unauthorised or illegal taking or releasing of data from a system, device, network, or other source. It involves deliberately stealing or obtaining sensitive, confidential, or personal information without permission, often for malicious or fraudulent purposes. A system breach by insiders refers to a scenario where staff with authorised access to a company's systems or networks intentionally exploit their privileges, provide backdoors, or create vulnerabilities to compromise the security of the system. This is mostly done in collusion with hackers and external fraudsters to gain access. The following are the subcategories and examples under this scheme:

- **Confidentiality breach:** Insiders may access and steal company, customer, agent or third-party data, including personal information from the mobile money system's databases. This stolen data can be used for identity theft, social engineering or to determine accounts with significant funds to be targeted by fraudsters. For example, staff with customer data access can identify high-value accounts, gather sensitive information, initiate unauthorised transactions, and transfer funds to other accounts.

- **Transaction manipulation:** Insiders with access to the transaction processing systems may manipulate transactions or divert funds by altering transaction records or rerouting money to their accounts or accomplices. An example of alteration of a mobile money account number is where an insider with system access manipulates and changes mobile money account number from legitimate number to fake registered MSISDN/phone number, before processing transaction to the fake account and withdrawing funds.

- **Override of controls:** Employees may use their privileged access to override security measures or access sensitive financial data and perform unauthorised transactions. For example, an employee overrides built-in security measures such as transaction limits and two-factor authentication requests that are normally sent to account holders for unusual activities, and transfers money from customer accounts.

- **Espionage:** Espionage by insiders refers to the act of employees with privileged access within an organisation gathering and sharing sensitive or confidential information with external parties to gain an advantage over - or to the detriment of - a mobile money provider. For example, an insider with access to encryption keys and security protocols collects sensitive data such as user information, such as accounts with high balances. The insider shares this information with an external fraudster who then targets the customer.

- **Sabotage:** These are deliberate actions taken by insiders to damage, disrupt, or hinder the operations of mobile money services. This can be motivated by various factors, including personal grievances and financial gain. An example of system tampering is where an insider intentionally introduces faults or errors including corrupting data, modifying software, or disrupting the network infrastructure, leading to service outages or incorrect transaction processing. Another example of sabotage is through spread of misinformation, where an insider spreads false information or rumours about the service, aiming to damage its reputation and trust among users.

This typology is unique because insiders are the gatekeepers with entrusted privileged access, knowledge and skills. This requires enhanced control measures and mitigation strategies, which are explained later in this report.

Insider fraud connections to other fraud categories

Impersonation schemes:
Insiders or individuals with authorised access to an organisation's systems, data, or resources, may use impersonation as a tactic to carry out fraudulent activities. This includes identity theft, where insiders steal the identities of colleagues or superiors to gain privileged access to sensitive information. This could involve using stolen physical access badges or login credentials, as shown in Figure 4 below. Insiders can also commit SIM swap fraud by exploiting their access to customer databases or systems to obtain personal information about the target, such as account details, phone numbers, and security questions crucial for convincing the mobile carrier to perform the SIM swap. Insiders may collaborate with external attackers by providing them with the necessary information or assisting in the SIM swap process. This could include sharing customer data, bypassing security controls, or facilitating communication with the carrier.

Cyber fraud:
These are schemes involving collusion between insiders and outsiders. Insider knowledge and privileges can be exploited to facilitate or execute hacking through unauthorised access to systems, networks, or databases, theft of login credentials, access codes, or encryption keys, insider threat collaboration, or data exfiltration. Insiders can also play a crucial role in facilitating man-in-the-middle (MitM), phishing, vishing, spoofing, cyber scams, and DOS attacks due to insider knowledge and access within an organisation.

4.4.3 Cyber fraud

This involves using vulnerabilities in technological systems, software, or hardware components, networks, or the internet in general to gain unauthorised access to commit fraud. In the context of mobile money fraud, this category includes attack vectors that exploit technical weaknesses such as software vulnerabilities, insecure network connections, and unauthorised access to devices. Subcategories include:

Hacking: Unauthorised access or manipulation of mobile money systems or accounts. It involves activities aimed at circumventing the security measures of mobile money platforms, often for malicious purposes and to the detriment of others. The following are subcategories of schemes under hacking:

- **Unauthorised access:** Hackers gain unauthorised access to mobile money accounts by exploiting vulnerabilities in the system, using techniques like phishing, social engineering, or exploiting software weaknesses. For example, hackers send out emails to a large number of mobile money users crafted to appear as if they are from the legitimate mobile money service provider. URLs in the message may redirect the user to a fake login page that closely resembles the real mobile money service login page. The page asks the user to enter their mobile money account credentials, including their username and password. Customers provide this information leading to unauthorised access to their accounts.

- **Transaction manipulation:** This involves unauthorised changes to financial transactions within the mobile money system.

- **Data breaches:** If there's a breach in the security of the mobile money service, personal and financial information of users could be compromised. This information could be used for identity theft or other fraudulent activities.

- **Malware used for hacking:** Hackers may deploy malicious software (malware) on mobile devices to compromise the security of mobile money transactions. This could involve keyloggers, screen capture tools, or other methods to capture sensitive information.

Man-in-the-middle attack: A type of cyberattack where a third-party intercepts and possibly alters the communication between two parties - usually the user and the mobile money service. In this scenario, the attacker positions themselves between the user's device and the mobile money system, allowing them to eavesdrop on or manipulate the data being exchanged. The following are subcategories under the man-in-the-middle attack:

- **Interception:** The attacker positions themselves between the user's mobile device and the mobile money service. The user's requests to the mobile money service and the responses from the service pass through the attacker's system.

- **Eavesdropping:** The attacker can eavesdrop on the communication between the user and the mobile money service. This may include capturing sensitive information such as login credentials, PINs and transaction details.

- **Injection of malicious content:** The attacker may inject malicious content into the communication stream. This could include injecting phishing pages or malware into responses from the mobile money service, leading the user to unknowingly download malicious software or enter sensitive information on fraudulent pages.

Denial-of-service (DoS):
Malicious activities that aim to disrupt or disable the normal functioning of mobile money services, making them temporarily or permanently unavailable to users. The goal of a DoS attack is to overwhelm the targeted system with an excessive volume of traffic, requests, or other forms of malicious activity, causing it to become slow, unresponsive, or completely unavailable. As discussed below, DoS occurs in the following forms:

- **Distributed denial-of-service (DDoS) attacks:** DDoS attacks involve multiple compromised devices, often forming a botnet, which simultaneously flood the targeted mobile money service with traffic.
- **Volume-based attacks (floods):** These attacks aim to flood the network bandwidth of the targeted system. They include Internet Control Message Protocol (ICMP) floods, User Datagram Protocol (UDP) floods, and other flood attacks that try to overwhelm the victim's network capacity.
- **Protocol and application-based attacks:** These exploit vulnerabilities in network protocols or application layer protocols to consume resources and disrupt normal operations.

Malware:
Malicious software designed to compromise the security and functionality of mobile devices and the mobile money applications or services they use. Different types of malwares pose various risks to mobile money transactions, personal information, and the overall integrity of financial systems. Malware is often used as a means of another scheme such as hacking, data-theft, sabotage or blackmail.

The following are subcategories of malware fraud schemes:

- **Trojans:** Trojans disguise themselves as legitimate software but contain malicious code. Once installed on a user's mobile device, they can intercept and manipulate mobile money transactions, capture login credentials, and potentially gain unauthorised access to financial accounts.
- **Viruses, worms and bots:** Viruses are programmes that can replicate themselves and spread to other files on the same device. They may corrupt or delete essential files, disrupt mobile money applications, or spread to other devices if mobile money apps are shared. Worms are self-replicating malware that can spread across devices and networks without user intervention. Worms can spread through messaging or other communication channels, potentially compromising the security of mobile money transactions. Bots are software that perform automated tasks.
- **Ransomware:** Ransomware encrypts a user's files or locks them out of their device, demanding payment to restore access. If mobile money service provider devices are infected with ransomware, users may be prevented from accessing information until a ransom is paid.

Phishing:
A type of cyberattack where attackers use deceptive methods to trick users into revealing sensitive information, such as login credentials, PINs, and other confidential details related to mobile money accounts. Phishing is typically carried out through various communication channels, such as emails, text messages, or fake websites, with the goal of impersonating legitimate entities to gain unauthorised access to financial information or conduct fraudulent transactions.

Spoofing:
A deceptive practice where attackers manipulate information to falsely represent their identity or the identity of a legitimate entity, such as a mobile money provider. The goal of spoofing is to trick users into believing they are interacting with a trustworthy source when in reality they are engaging with a malicious actor. Spoofing can occur through various communication channels, including emails, text messages, phone calls, and websites.

Some of the phishing and spoofing schemes in mobile money include email phishing and spoofing, spear phishing, and caller ID spoofing. There are many other phishing and spoofing schemes with a unique approach, but they all share the common approach. Below are some subcategories:

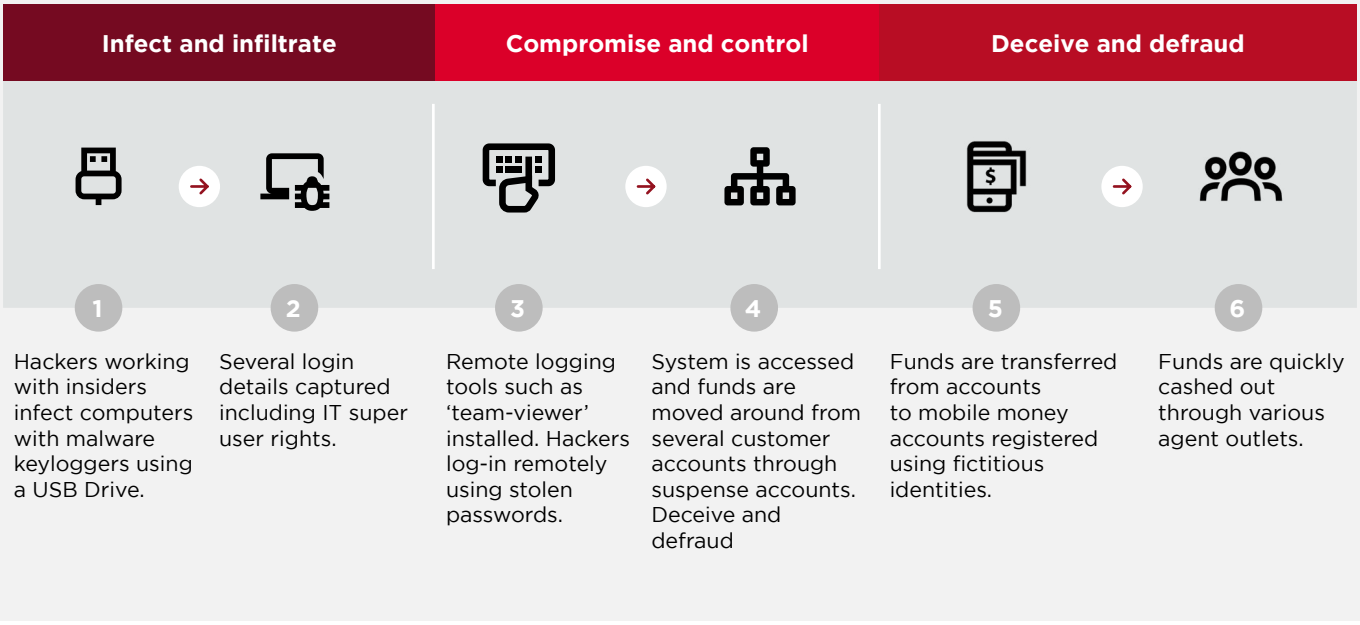
Email phishing:
The most common form, where attackers send fraudulent emails impersonating legitimate organisations to steal sensitive information. sensitive information or follow instructions that lead to fraudulent transactions.

Spear phishing:
A targeted form of phishing, where attackers customise their approach for specific individuals or organisations, often using personal information to seem more convincing. For example, attackers research and identify an executive and gather personal information about him and craft a convincing email that appears to come from a trusted professional contact. The email references a recent conference the person attended and asks him to review the information in the link. The person proceeds to click the link leading to attack.

Caller ID spoofing:
Attackers manipulate the caller ID information to display a phone number that appears legitimate, such as that of a bank or mobile money provider. Users may receive calls that seem to be from a trusted source, prompting them to provide sensitive information or follow instructions that lead to fraudulent transactions.

Although we have categorised various schemes, they are seldom executed in isolation, as shown in the illustration below:

Figure 4: An example of mixed scheme fraud



Cyber fraud connections to other fraud categories

Insider fraud:
Insiders collude with external hackers to orchestrate a data breach. They may provide access to sensitive databases, credentials, or other insider information to facilitate the theft of valuable data.

Impersonation schemes:
Cyber fraud schemes such as phishing, vishing, and spoofing are specific tactics used to carry out social engineering. Cybercriminals may target individuals' personal information to steal their identities and then use that stolen identity to commit various forms of fraud, such as unauthorised financial transactions, opening credit accounts, obtaining government benefits, or engage in SIM swap fraud.

4.4.4 Agent Fraud

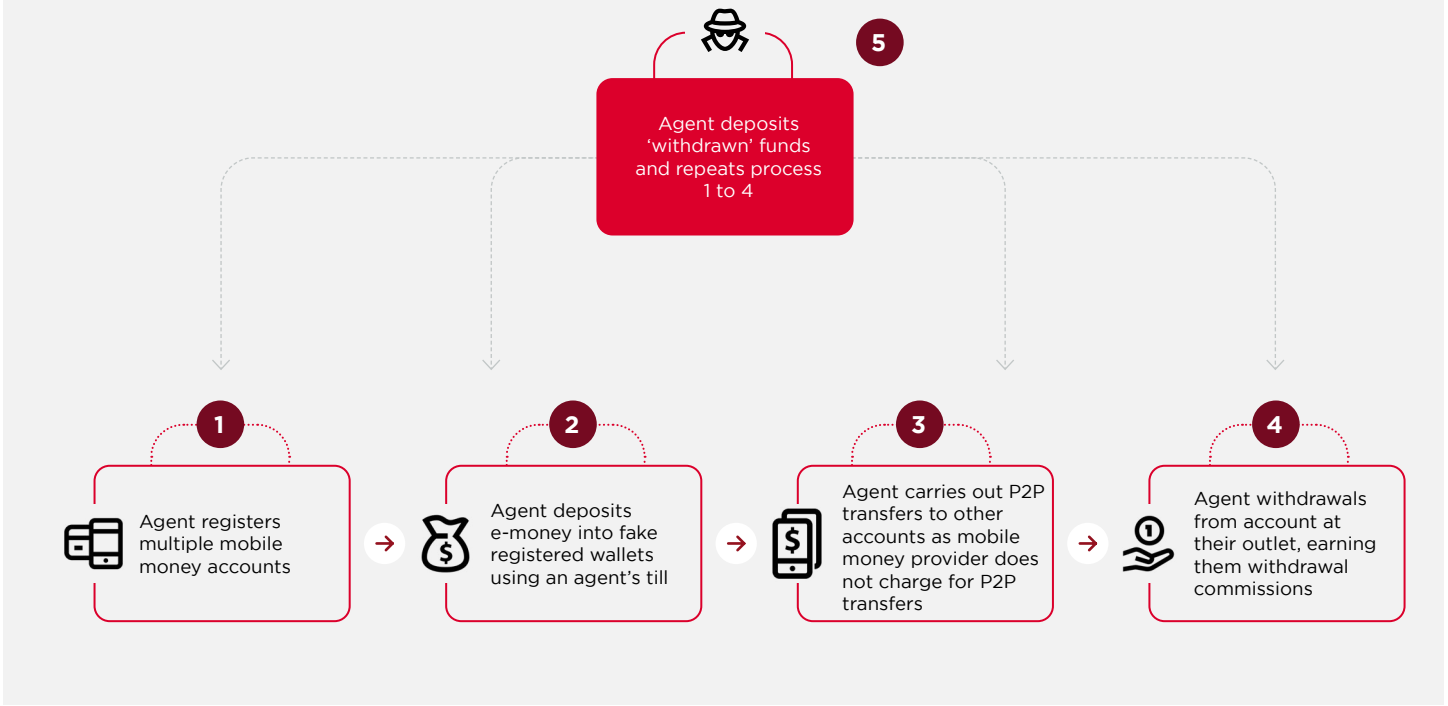
This is fraud committed by agents. An agent is a person or business that serves customers on behalf of a mobile money provider. They provide the mobile money provider with a wide distribution network and perform various functions including deposits (cash-in), withdrawals (cash-out), SIM registration and KYC verification for opening mobile money accounts.

Agents are embedded within - and mostly belong to - communities they operate in. This means that they can easily build trust with customers - this trust can be exploited to commit fraud.

In the context of mobile money fraud, this category includes:

Commission fraud:
Agents earn commissions through carrying out transactions. The primary value proposition and motivation of one becoming an agent is to earn money in the form of commissions. Agents look for opportunities to maximise their commissions. Commission fraud is the earning of commissions through arbitrage by manipulating or exploiting the commission structure, system and/or process loopholes to fraudulently increase earnings. Commissions fraud involves agents exploiting each other. Our survey found that commissions fraud is the highest fraud scheme among agents. The chart below illustrates an example of commission fraud - in this example, a mobile money service does not charge for peer-to-peer (P2P) transfers among customers:

Figure 5: The process of commission fraud



The following are subcategories and examples of fraud schemes under commission fraud:

Split transactions: This is the splitting of deposits or withdrawals to earn more money from commissions. For example, when a customer deposits $250, it may earn an agent $2 in commission. If the agent splits the transaction in two at $125 each, they can earn $1.50 for each, bringing the total to $3. In such scenarios, the agent may tell the customer that the agent account cannot accept the $250 as a single transaction due to a 'technical limit', and the customer agrees to split the transaction.

Topping-up transactions: This is where an agent asks a customer to increase the transaction value to move the amount into the next bracket. For example, a mobile money provider has a withdrawal commission tariff where an agent earns $0.45 for a withdrawal of $150. However, for a withdrawal of $150.10 the agent earns $0.70. In this situation an agent may request the customer to withdraw $150.10. If the customer agrees, the agent earns extra commission.

Arbitrage by circulating funds: This is moving funds around, depositing and withdrawing them, taking advantage of gaps in the processes to earn more commissions. This is demonstrated in figure 5, above. An example of arbitrage by deposits and withdrawals using fake accounts is where an agent deposits funds in fictitious accounts and proceeds to transfer money to other accounts before withdrawing the funds, thereby earning withdrawal commissions for illegitimate transactions.

Super or master agents defrauding sub-agents: This is where a super or master agent does not disclose the correct commission percentage and pays less commissions to sub-agents. An example is where the master agent withholds part of commission payable to sub-agents. For example, a sub-agent who should receive 95% of commissions paid on transactions at the till can be denied this by the master agent who may withhold most or all of the commission owed to the sub-agent.

Cash-in cash-out (CICO) fraud schemes: These are embezzlement schemes by agent staff on customers at CICO points. They typically involve short-changing the customer by giving less cash during withdrawals, depositing less e-money, making fraudulent transfers, or engaging in fake currency schemes. Agents exploit customer trust, lack of attention and low literacy levels to defraud them.

The section below shows the schemes at CICO points which exploit customer trust, lack of attention and low literacy levels to defraud customers:

Withdrawal fraud: This occurs when an agent gives the customer less cash than what has been withdrawn. For example, a customer visits an agent to make a withdrawal. The agent initiates and completes withdrawal. They give the customer cash in many low denominations, which are time-consuming or difficult to count. The customer signs an agent transaction book without counting and confirming cash amount.

Deposit fraud: This involves receiving less e-money than the physical cash handed over by customer to agent. For example, a customer visits a local mobile money agent to deposit cash into their mobile money account. They hand over 5,000 units of their local currency to the agent with the intention of having the same amount credited to their mobile money account. The agent however deposits 4,500 units. When the customer notices, the agent may promise to send the balance but fail to do so.

Fraudulent or irregular transfers: Here, an agent takes advantage of customers by initiating transfers from the customer wallet to other number(s) and deleting confirmation messages before customer realises the transfer has taken place. This happens through social engineering. An example is where a customer visits an agent to perform a transaction. The customer trusts agent and has low literacy levels. They hand their phone to the agent to assist in performing the transaction. The agent performs the transaction but also carries out a P2P transfer while distracting customer before deleting the transaction messages.

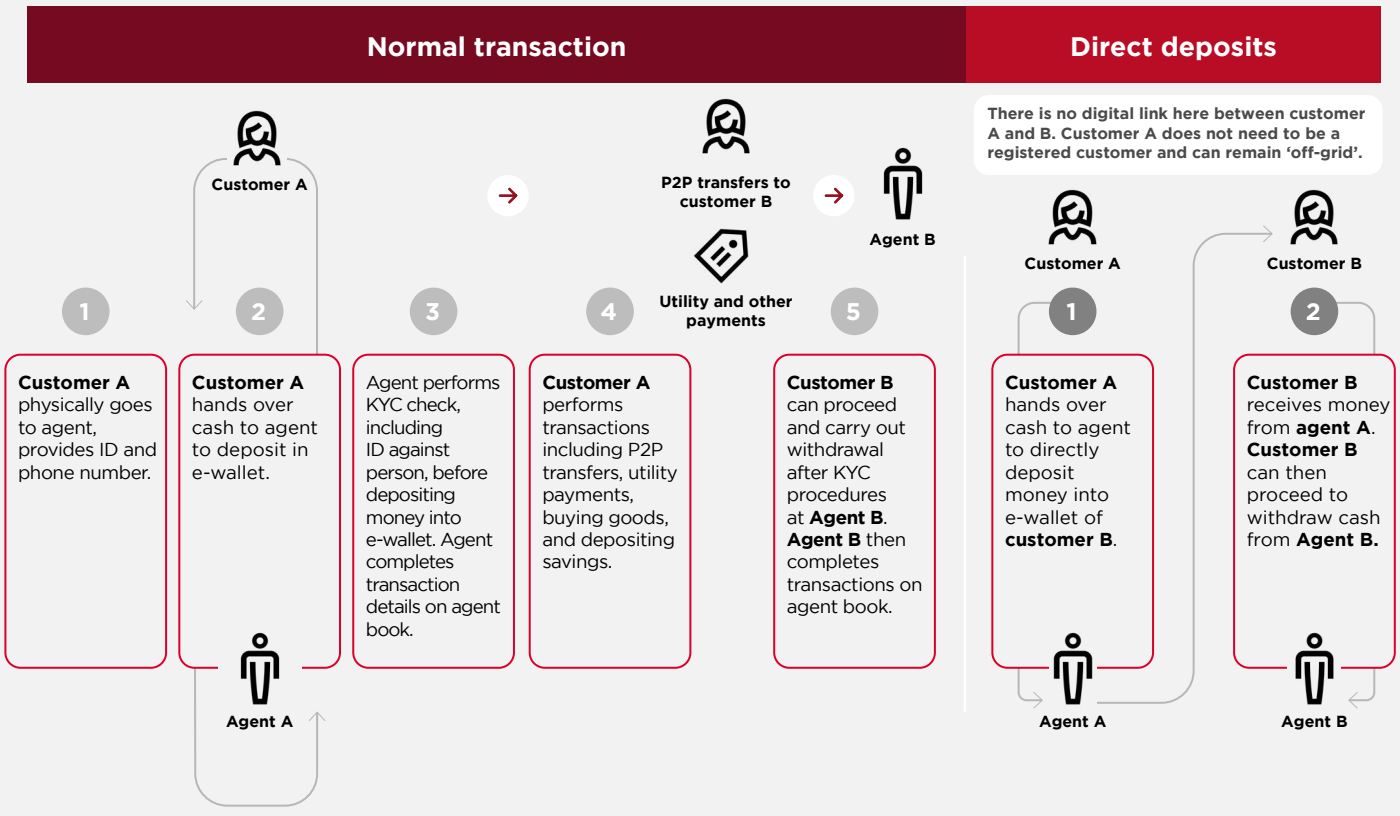
Counterfeit currency schemes:
This is when an agent gives or receives counterfeit currency at a CICO agent outlet. An example is when an agent assistant receives fake currency and knowingly accepts it to defraud their employer. Another example is where an agent assistant gives fake currency.

Illegal fees and services:
Agents can charge illegal fees and services. This can take the form of services that should be free or are non-existent. Subcategories and examples of illegal fees and services are as follows:

- **Electronic information breaches**: This is when information in electronic form from the customer's account is unknowingly and illegitimately accessed by the agent. This information is typically contained on an agent device or customer phone. For example, an agent may shoulder-surf a customer on their phone to obtain a PIN or account balance.
- **Transaction book or receipts breaches:** This is information on a customer transaction book or receipt kept by the agent. An example is when an agent sells to customer information to fraudsters who use it for social engineering.

KYC breaches:
This is where a mobile money agent fails to follow the KYC protocols. This includes carrying out 'direct' deposits and withdrawals in cases where customers have not been verified with any form of identification. An illustration of normal transactions vis-à-vis direct deposits can be found below:

Figure 6: MMU spotlight on direct deposits



Examples of schemes subcategorised as KYC breaches include:

Direct deposit: This occurs when the customer initiating a P2P transfer hands the agent cash but provides them with the mobile number of the recipient rather than their own. The agent deposits the funds directly into the recipient's account. In doing so, the agent has essentially turned a mobile wallet service into an over the counter (OTC) transfer service. Figure 6 above compares regular, proper e-wallet transactions and direct deposits. An example is where a customer would like to send money to another person without their disclosing their details. They pay the agent to carry out a direct deposit to the recipient - the recipient receives the e-money from agent as if they were physically present at the outlet, when they were not.

Remote withdrawal: This is the reverse of a direct deposit where the customer does not appear before the agent and identified themselves. They initiate the transaction remotely and the cash is collected by another person at the outlet. For example, a customer wants to pay for illicit goods or services without being directly linked with the seller. They initiate a mobile money withdrawal transaction remotely, and seller collects the cash at the agent's outlet.

Poor customer identification: This happens when customers fail to properly identify themselves when carrying out CICO transactions at the agent outlet. This enables other fraud schemes such as social engineering. For example, a customer goes to an agent outlet to carry out withdrawal. The customer claims they forgot their ID card. The agent allows the customer to carry out the withdrawal - however, this customer is a fraudster who has performed an account takeover of someone else's mobile account.

Cash-in cash-out (CICO) fraud schemes: These are embezzlement schemes by agent staff on customers at CICO points. They typically involve short-changing the customer by giving less cash during withdrawals, depositing less e-money, making fraudulent transfers, or engaging in fake currency schemes. Agents exploit customer trust, lack of attention and low literacy levels to defraud them.

Agent fraud in connection with other fraud categories

In impersonation schemes, agents can deceive a customer or engage in shoulder-surfing to gain access to a PIN or other sensitive information. This can be used to perform a SIM swap and account takeover. Shoulder-surfing is a type of social engineering technique used to obtain information such as PINs, passwords and other confidential data by looking over the victim's shoulder. Because some providers allow agents to carry out SIM registration, they can also carry our identity fraud and theft such as registering fictitious mobile money accounts.

In insider fraud, agent staff can carry out embezzlement against their employer, the agent, or carry out fraud on a mobile money provider. Master or super-agents can engage in corruption schemes by abusing their position for personal gain. For instance, they can sell tills and other assets for free that are given by the provider to sub-agents. Agents have access to confidential information which can be abused. For instance, they have access to transaction books and receipts that may contain information that can be used to socially engineer customers.

4.5 Trends and patterns in mobile money fraud

Mobile money has had significant socio-economic impact with a $1.26 trillion transaction value and 1.6 billion registered mobile money accounts in 2022.[13] Across the world, mobile money services are growing - and fast. It took the industry 17 years to reach the first 800 million customers, but only 5 years to reach the next 800 million, and of that, 400 million accounts were added over the course of the COVID-19 pandemic.[14] There is also a substantial increase in mobile application transactions between 2019 and 2020. At the same time, fraudulent activities such as mobile app fraud, SIM swap fraud, account takeovers, and social media scams continue to challenge the industry and customer alike.[15]

Mobile payments are growing significantly in developing economies. Mobile-based money transfers allow users to access financing and micro-financing services, and to easily deposit, withdraw and pay for goods and services with a mobile device. In some cases, almost half the value of some African countries' GDP goes through mobile phones. However, this is threatened by an increase in fraud in digital financial services (DFS). For instance, Brazil and Mozambique experience a high rate of SIM swap fraud. In Mozambique, one bank had a monthly average of 17 SIM swap cases; in Brazil, 5,000 people fell victim to SIM swap fraud.[16]

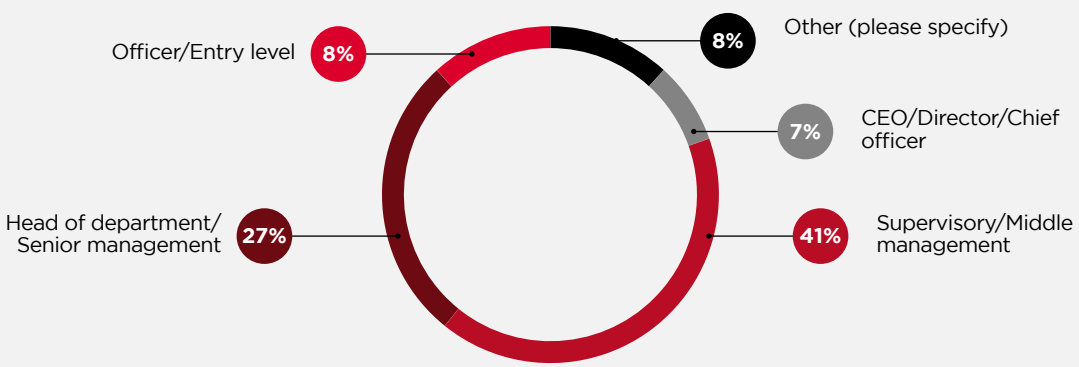
The DFS Consumer Risk Typology framework is a CGAP categorisation of identified DFS risks that uses a risk-based approach to categorise threats to digital finance. This includes some aspects of mobile money fraud, such as agent fraud.[17] This research shows an increase in scale for most of the risk types identified by CGAP since 2016.

After research and reviewing available literature, the GSMA sought to conduct more research on trends and patterns in mobile money fraud. The survery included responses from 8 industries in the mobile money ecosystem from 34 countries in Africa, Latin America and Asia.

ACFE conducted a survey asking respondents about their current observations regarding the overall level of fraud in the wake of COVID-19. As of May 2020, 68% of survey respondents had already experienced or observed an increase in fraud, with one quarter reporting the observed increase had been significant. This analysis is particularly useful since fraud observed during and after COVID has been digital in nature and through digital financial services channels. This is because the pandemic accelerated use of digital channels for financial transactions and work-based functions. The survey further shows that fraud perpetrated by vendors and sellers (for instant integrators and technology service providers) are a top risk in the wake of the COVID-19; 86% of respondents expect to see more of this type of fraud over the coming years. Payment fraud which includes mobile payments ranked as the third most likely type of fraud expected to increase over the coming year.[18]

After research and reviewing available literature, the GSMA sought to conduct more research on trends and patterns in mobile money fraud. The survery included responses from 8 industries in the mobile money ecosystem from 34 countries in Africa, Latin America and Asia.

Figure 7: Demographic of the survey participants



13 GSMA State of Industry Report (SOTIR) for Mobile Money 2023
14 Raithatha, R., et al. (2023). The State of The Industry Report on Mobile Money. GSMA
15 Chalwe-Mulenga, M., Duflos, E., & Coetzee, G. (2022). The Evolution of the Nature and Scale of DFS Consumer Risks: A Review of Evidence. CGAP
16 Assolini, Fabio, and Andre Tenreiro. 2019. "Large-scale SIM Swap Fraud." Securelist research.
17 Chalwe-Mulenga, M., Duflos, E., & Coetzee, G. (2022). The Evolution of the Nature and Scale of DFS Consumer Risks: A Review of Evidence. CGAP
18 Ibid

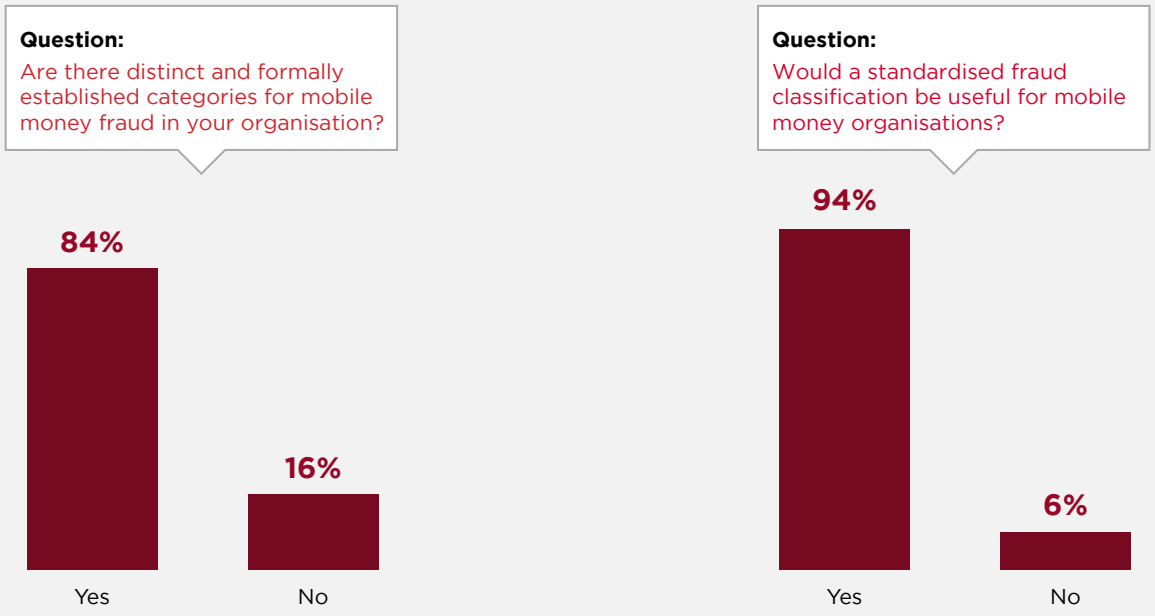
Our survey targeted professionals in the mobile money ecosystem with significant knowledge and experience of mobile money fraud. The distribution of respondents of this survey leans towards middle-to-senior management roles (76.47%), with fewer participants in entry-level positions (11.76%). Others, largely consultants and advisors, make up the remaining 11.76%. All-in-all, the survey was undertaken by experienced professionals. This is particularly important as we found that mobile money and fraud are both highly technical subjects. For instance, during our research, we found that many customers did not clearly understand what cosnstitutes fraud. For example, some classified all scams and theft they encountered where money is paid through any electronic wallet or app, as mobile money fraud.

Although 50.98% of respondents to the survey were mobile money service providers, the remaining percentage (49.02%) was spread among finanical insititutions such as banks, IT service providers, integrators, fintechs, savings and credit cooperatives, consultants, regulators, and multilateral institutions. This indicates that the survey reached a diverse range of stakeholders and industries, and featured strong participation from mobile money providers, who are the key player in the mobile money ecosystem .

The countries that contributed to this survey are Kenya, Tanzania, Uganda, Ethiopia, South Sudan, Somalia (including Somaliland), Malawi, Zambia, Seychelles, DRC, Congo Brazzaville, Gabon, Nigeria, Ghana, Niger, Rwanda, Madagascar, Chad, Cameroon, Ivory Coast, Madagascar, Lesotho, South Africa, Liberia, Mozambique, India, Pakistan, Bangladesh, Myanmar, Colombia, Philippines, Paraguay and Honduras. These are markets with significant mobile money deployments.

4.5.1 Importance of standardised fraud classifications in mobile money

Figure 8: Survey responses on fraud classification in organisations



As shown above, 84.31% of respondents indicated they had formally established categories in mobile money fraud. The data strongly suggests that formal categorisation of mobile money fraud is a common practice in mobile money, which could reflect a proactive stance in dealing with fraud in the mobile money financial services sector. 15.69% of respondents report that their organisation does not have such categories formally established. During our interviews, we found that although some mobile money providers have forms of categorisation, these are not formally established in policy.

An overwhelming majority, 94.12% of respondents, believe that a standardised fraud classification would be useful for mobile money fraud. This indicates a strong consensus that a standardised system could potentially improve the management, reporting and mitigation of mobile money fraud. A small minority, 5.88%, do not believe a standardised fraud classification would be useful. This could be due to various reasons, including the uniqueness of fraud patterns or possible concerns about the complexity and implementation challenges of a standardised system. Our reseach has found the following as potential benefits of standardisation:

- **Consistency**: It ensures that all instances of fraud are categorised consistently across the organisation, which is crucial for accurate reporting and analysis.
- **Communication**: It facilitates clearer communication within an organisation and with external partners, including law enforcement, regulators, and other financial institutions.
- **Efficiency**: Standardisation can streamline the process of fraud detection and management, making it more efficient and less prone to error.
- **Benchmarking and metrics**: It allows for better benchmarking and metrics, as fraud cases are comparable across different departments or even across different organisations and industries.
- **Training and awareness**: It aids in training and raising awareness among staff by providing clear definitions and examples of what constitutes fraud in different categories.
- **Improved analytics**: Standardised data can be more easily analysed to detect patterns and trends in fraudulent activities, which can lead to more effective predictive measures.
- **Cross-industry collaboration**: It encourages collaboration and sharing of best practices across the industry, helping organisations to use similar frameworks for dealing with fraud.
- **Resource allocation**: Organisations can allocate resources more effectively when they understand the types of fraud that are most prevalent or most damaging.
- **Customer trust**: It can increase customer trust, as customers may feel more secure knowing that there is a standardised system in place to protect against fraud.
- **Adaptability**: A standardised system can be designed to be flexible and evolve as new types of mobile money fraud emerge.

4.5.2 Impersonation and insider fraud are most prevalent fraud schemes

This diagram indicates which fraud schemes respondents considered to be the most prevalent in mobile money:

Figure 9: Survey response on most prevalent fraud schemes

Impersonation schemes rank the highest with identity fraud being the most prevalent type of mobile money fraud scheme at 90.38%. This is followed by social engineering schemes at 88.46% and another impersonation scheme, SIM swap fraud, ranking fourth at 78.85%. Insider fraud ranked third at 86.54% and cyber fraud ranking fifth at 59.62%. Commissions fraud, an agent fraud scheme, ranked sixth at 55.77%.

4.5.3 Insider fraud and collusion between internal and external actors

The overwhelming majority of respondents, 94.12%, indicated that the most common mobile money fraud they encounter involves both internal and external actors. This suggests that most fraud cases they deal with are not limited to either external parties such as hackers, or internal staff such as employees, but a combination of both. It could imply collusion between internal and external parties.

Furthermore, 88.24% of respondents indicated collusion with external fraudsters as the most prevalent type of insider fraud and threat issue, as shown in the graph below. This indicates that internal parties are often working in concert with outside individuals to commit fraud:

Figure 10: Survey responses on the types of internal fraud in their organisation

Question:

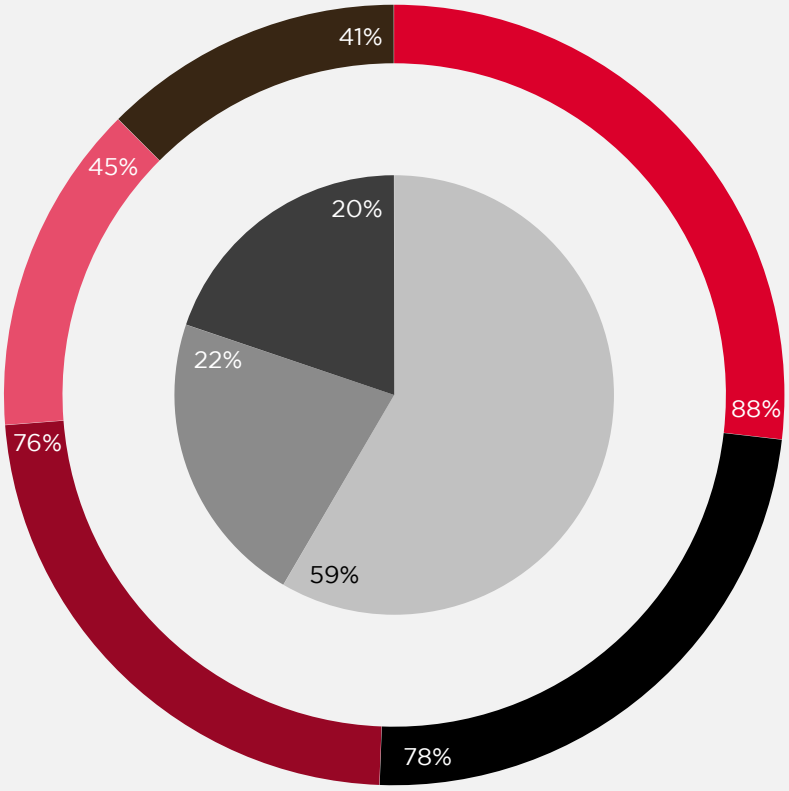
Which of the following are key types of internal fraud your organisation encountered?

- Collusion with external fraudsters
- Embezzlement
- Data theft and system breach
- Conflicts of interest
- Bribery

Question:

Are there distinct and formally established categories for mobile money fraud in your organisation?

- Sometimes
- Often
- Rarely



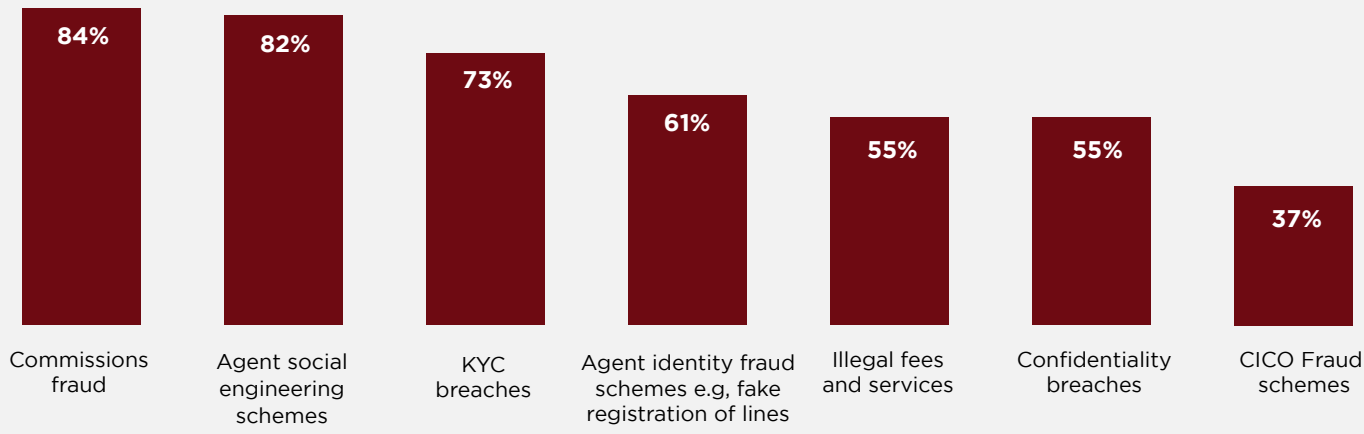
This is further supported by the question on frequency of involvement of staff of third-party service providers, such as technology vendors. The majority of the respondents, 58.82%, reported that they are sometimes involved, and 21.57% said they are often involved. This indicates that this happens with enough frequency to be notable and reinforces the importance of investigating more deeply into insider fraud.

In addition, 54.90% of respondents indicated they encounter mobile money being used as a conduit for fraud at least every month. These are instances where the actual fraud is not related to mobile money. An example would be an investment fraud or ponzi scheme that receives payments through mobile money, or bank hackers that use money mules in mobile money, along with other multi-channels, to exit funds.

4.5.4 Agent commission (arbitrage) fraud

As indicated below, the highest agent fraud scheme is commission (arbitrage) fraud. It is also indicated as among the overall most prevalent fraud schemes in mobile money at 55.77%. Agent social engineering schemes come second at 82.35% and agent identity fraud schemes, such as fake registration of SIM/ MSISDNs, coming fourth at 60.78%. These results are consistent with his report's taxonomy and typology sections whch indicate a link between agent fraud and impersonation schemes, in particular, social engineering and identity fraud.

Figure 11: Survey responses on the different agent fraud schemes

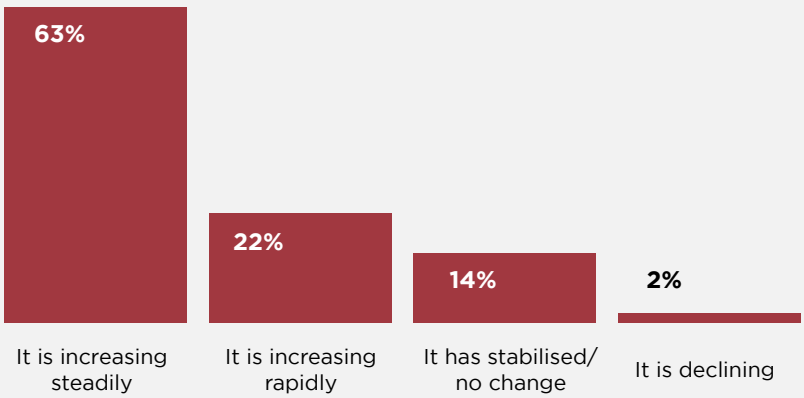


KYC breaches remain a major issue, coming third at 72.55%. These include direct deposits, remote transactions and failure to identify customers properly during CICO transactions.

4.5.5 Impact of mobile money fraud

21.57% of respondents indicated that fraud was increasing rapidly while 62.75% indicated that it is increasing steadily - a combined total of 84.32% that believe fraud is generally increasing, as shown in the graph below. The average estimated loss of funds due to mobile money fraud annually per mobile money provider is $1.06 million:

Figure 12: Survey responses on the increase of mobile money fraud



Estimated annual loss per mobile money provider

$1.06M

The average annual loss of $1.06 million represents 0.03% of the average transaction volume per provider. (GSMA SOTIR 2022 $1.26tn / 315 deployments globally).[19] However, it should be noted that some mobile money fraud cases can lead to losses far more significant than the average losses reported by our respondents. However, the impact of fraud can be greater than pure financial losses, as indicated below:

Deterioration of trust: Any compromise in trust may lead to reluctance in using the services, adversely affecting the provider's reputation.

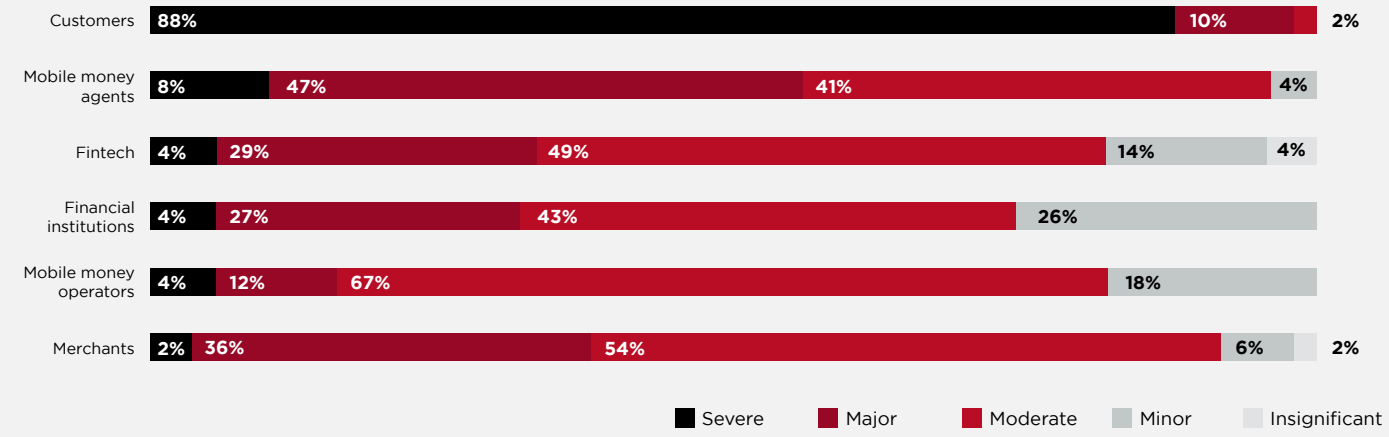
Competitive disadvantage: Users are less likely to opt for services perceived as less secure and reliable, potentially resulting in a loss of market share.
Brand impairment: The occurrence of fraud incidents can result in damage to the provider's brand. Users experiencing financial losses or disruptions due to fraud can become dissatisfied with the mobile money service provider.

Legal and regulatory scrutiny: Stricter requirements, audits, or penalties imposed by regulators can exacerbate the service provider's damaged reputation within the industry.

Disruption of services: Incidents of fraud may lead to disruption as providers implement emergency responses. These include conducting investigations and addressing security vulnerabilities, both of which hinder the provider's ability to deliver services seamlessly.

We further asked respondents who had been most severly impacted by mobile money fraud:

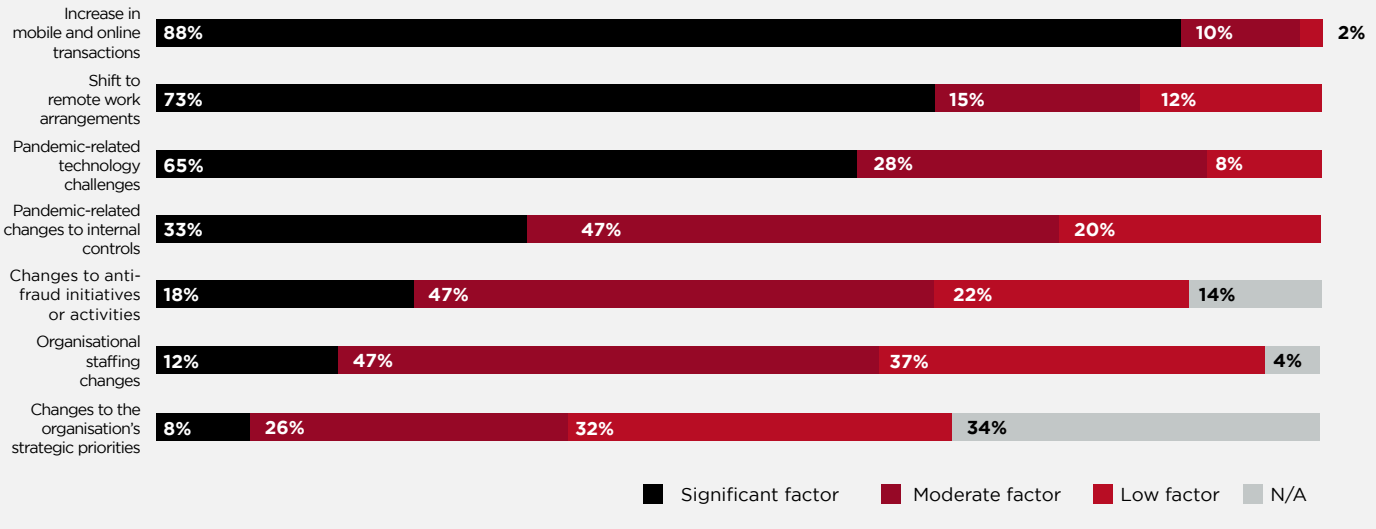
Figure 13: Survey responses on the most severely impacted by mobile money fraud in the mobile money ecosystem



4.5.6 Post-COVID factors contributing to increase in fraud

We asked to what extent have the following post-COVID factors contributed to an increase in mobile money fraud:

Figure 14: Survey response on post-COVID factors contributing to an increase in mobile money fraud

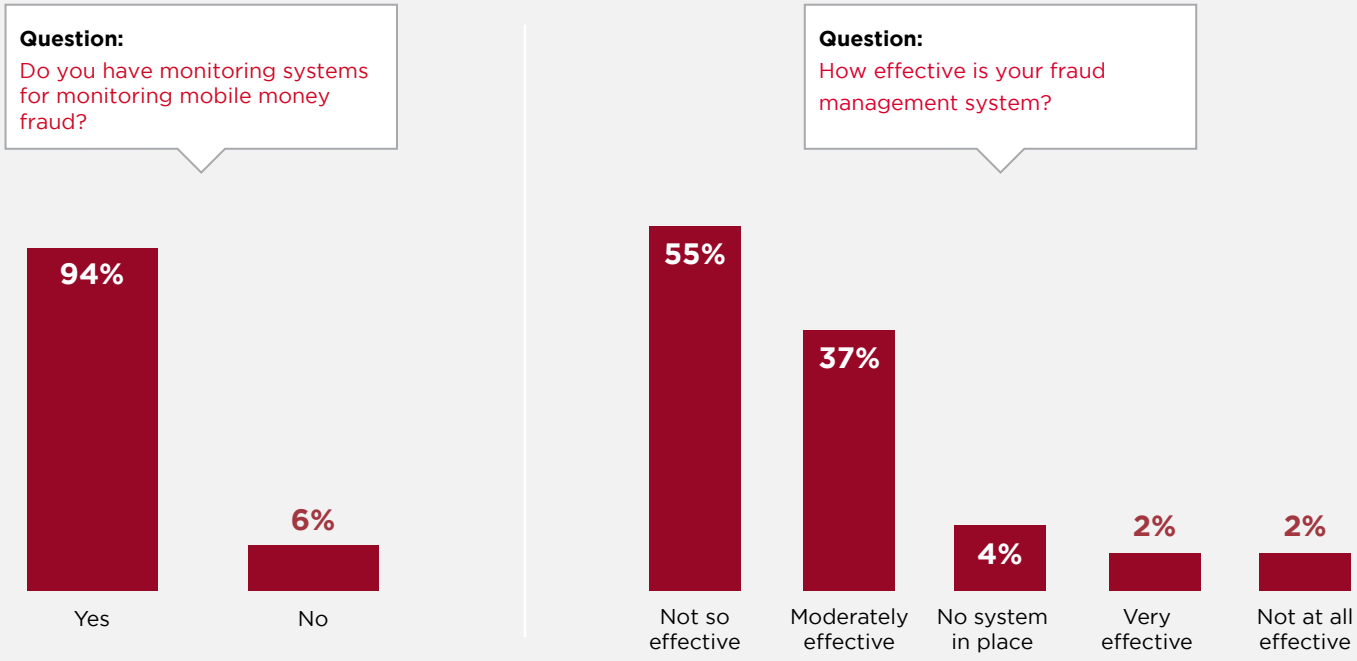


19 GSMA State of Industry Report (SOTIR) for Mobile Money 2022

The main post-covid factors contributing to the increase in mobile money fraud is increase in mobile and online transactions (88.24%), shift to remote work arrangements (72.55%) and pandemic-related technology challenges (64.71%). These are likely due to a dramatic shift in business and consumer behaviour towards mobile and cashless payments and remote work arrangements. This resulted in a surge in mobile and online financial activities. The rapid increase in the volume of transactions may have provided more opportunities for fraudsters to exploit new ways of working and transacting. Additionally, many systems were quickly scaled up to accommodate the increased load, which may have led to certain process and technological vulnerabilities.

4.5.7 Anti-fraud systems and controls

Figure 15: Survey responses on fraud management systems in their organisation

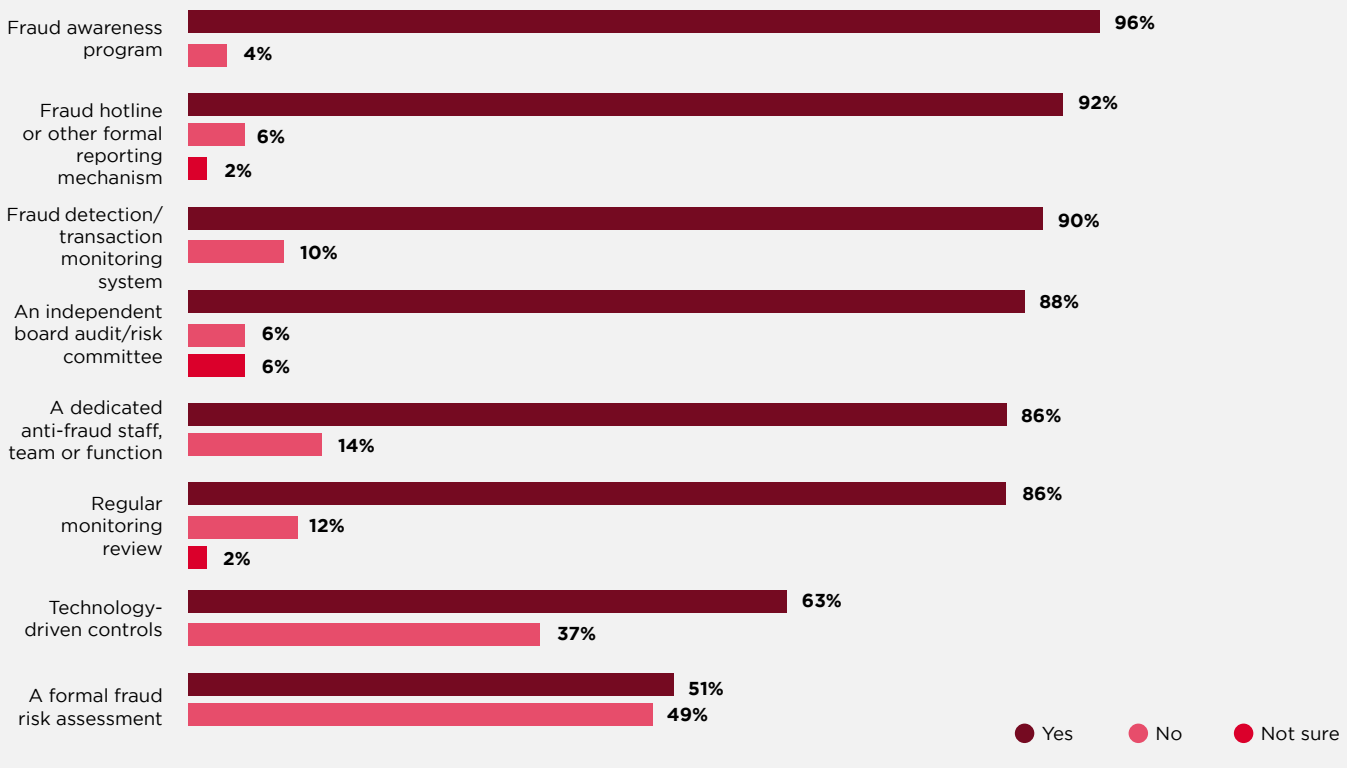


A vast majority of respondents at 94.12% affirm that they have systems in place for managing mobile money fraud. This high percentage indicates that most organisations recognise the importance of specialised systems in the prevention, detection and investigation of mobile money fraud, and have invested in their implemention.

However, the majority of respondents at 54.90% also feel that their fraud management systems are not so effective. This could indicate that while systems are in place, they may not adequately address fraud, or that the nature of fraud has evolved beyond the capacity of current systems.

In addition, we asked respondents to indicate whether they had the following general anti-fraud controls - they responded as follows:

Figure 16: Survey responses on anti-fraud controls



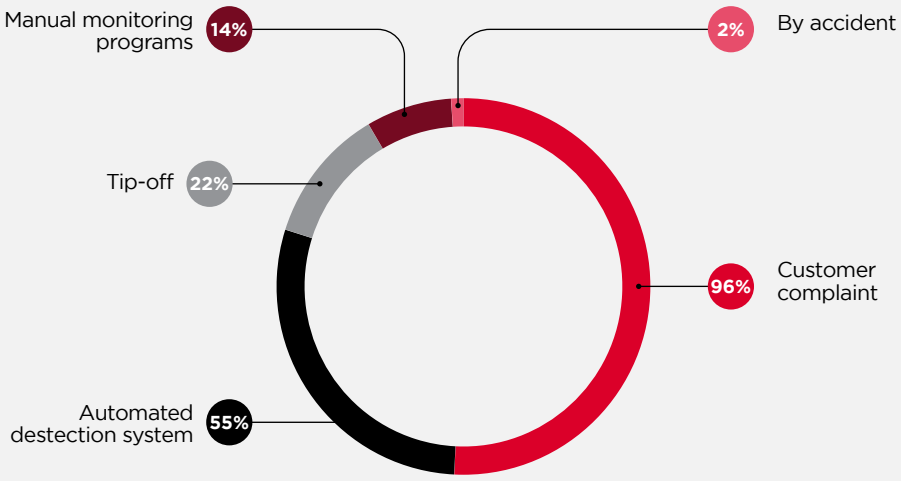
Overall, these controls suggest that organisations are serious about combating fraud and have invested in a multifaceted approach that includes awareness and training, detection and monitoring systems, appropriate functions and staff, and a reporting and governance structures that create a robust defense against fraud.

However, close to half of respondents (49.02%) have not conducted a formal fraud risk assessment. Without it, mobile money players may not be fully aware of all the potential fraud risks they face, leaving them vulnerable to attacks they have not anticipated or prepared for. In addition, it may lead to ineffective controls, as organisations may instead allocate resources to controls that address minor exposures rather than critical risks, leading to ineffective anti-fraud programs.

4.5.8 Customer recourse and reporting channels

We asked respondents how they generally detect mobile money fraud. The graph below indicates that an overwhelming majority of fraud (96.08%) is detected through customer complaints.

Figure 17: Survey responses on fraud detection in organisations

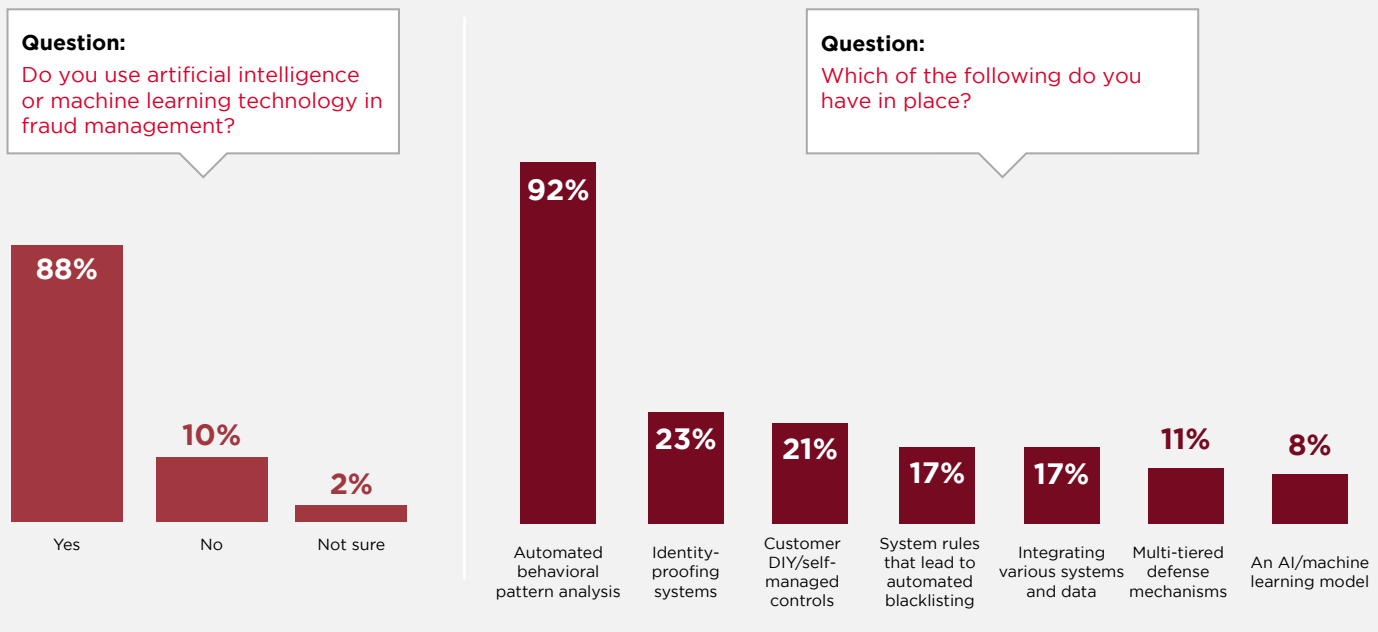


This indicates that customers are often the first to notice and report fraudulent activity on their accounts. The high percentage of fraud detection through customer complaints also suggests that customers are aware of the channels available to them for reporting fraud, and that they are using these channels effectively. This could also imply that mobile money providers have established and communicated proper reporting channels to their customers.

The data may also reflect a reactive stance towards fraud detection, heavily reliant on reports after the fact, and highlights the importance of having robust detection mechanisms in place. It also underlines the importance of customer service and complaint management systems in the fraud detection process.

We also asked respondents about their use of latest technologies and approaches:

Figure 18: Survey responses on deployment of latest technologies in fraud



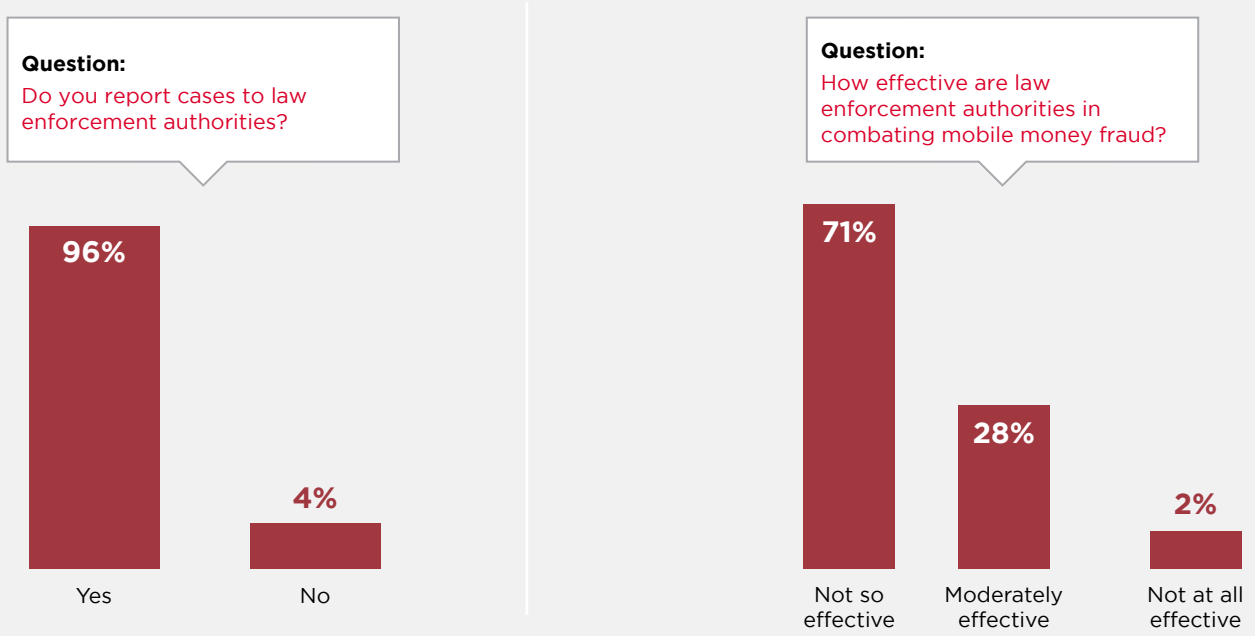
The majority of respondents (91.67%) use automated behavioural pattern analysis. This high percentage suggests a widespread adoption of rule-based systems capable of detecting anomalies in behaviour patterns which may indicate potential fraud.

However, it also highlights that more advanced AI and machine learning models and other detection and prevention mechanisms are largely not in place. It suggests that while there is an awareness of high-tech solutions, the actual deployment of such advanced systems is not yet widespread.

4.5.9 Law enforcement authorities and regulators

The majority of respondents (96.08%) report cases of mobile money fraud to law enforcement authorities, as shown below. This indicates a strong adherence to regulatory and legal requirements and also a proactive approach by mobile money players in seeking justice and building deterrence against future occurences of through official channels. However, a significant majority of respondents at 70.59% feel that law enforcement authorities are not so effective in combating mobile money fraud, as shown below:

Figure 19: Survey responses on the effectiveness of law enforcement authorities in combating mobile money fraud



Key factors contributing to ineffectiveness are indicated in the question “if not effective, what are the contributing factors to their ineffectiveness?”:

Figure 20: Survey responses on key factors contributing to the effectiveness score of law enforcement authorities

96% of respondents identify lack of technical capacity as a key factor to law enforcement ineffectiveness

96% of respondents identify lack of technical capacity as a key factor to law enforcement ineffectiveness. This suggests that there is a view that law enforcement authorities may not have the specialised skills needed to effectively investigate and combat mobile money fraud. A significant majority (84%) also believe that inadequate resources are a contributing factor. This could mean that there is insufficient funding, manpower, or equipment for law enforcement to address mobile money fraud effectively.

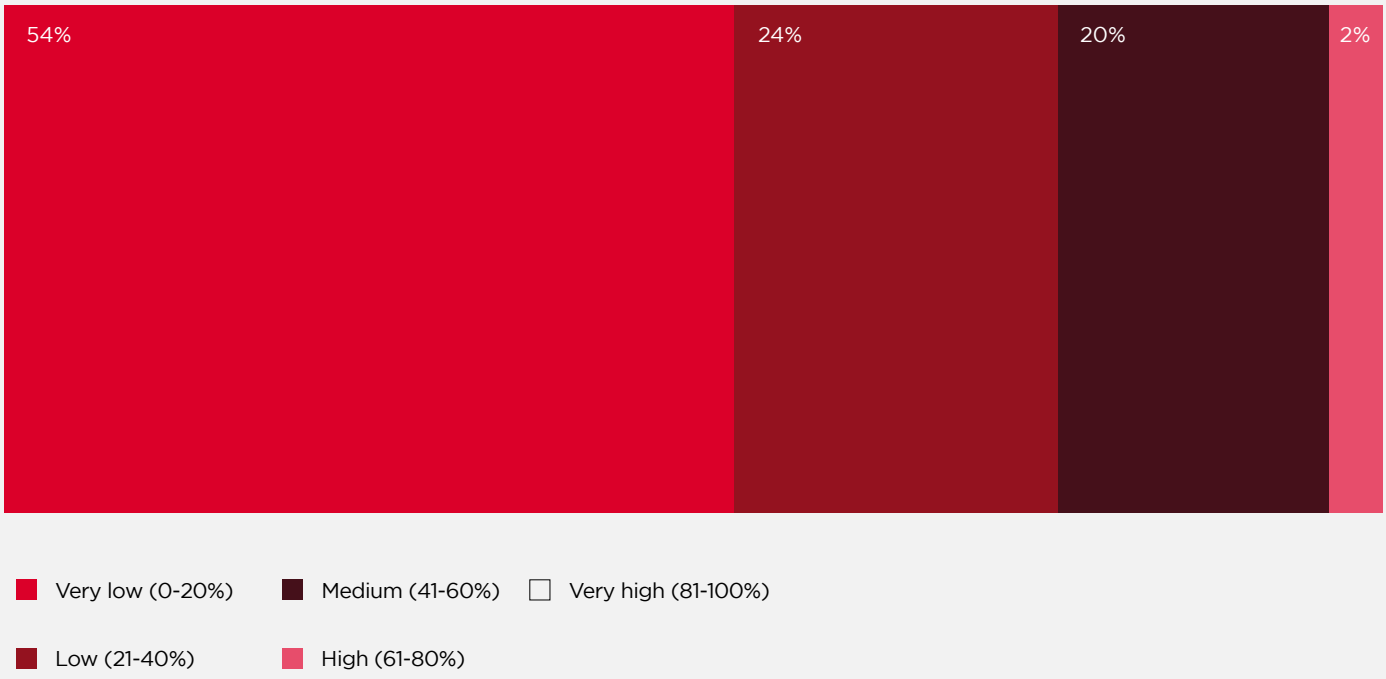
Over half of the respondents (54%) cite corruption within the police force as a factor, implying that unethical practices among law enforcement officials could hinder fraud investigations and prosecutions.

A third of the respondents (34%) point to the absence of adequate legal frameworks as a problem, indicating that existing laws in their countries may not be robust enough to deal with the nuances of mobile money fraud.

Further, we asked what percentage of fraud cases have been successfully concluded. We found that a majority of mobile money fraud cases at 78% have a low or very low conclusion rate, as indicated in the below chart.

This may contribute to an increase in fraud cases since offenders are not being sufficiently dealt with, emboldening others due to a lack of deterrence.

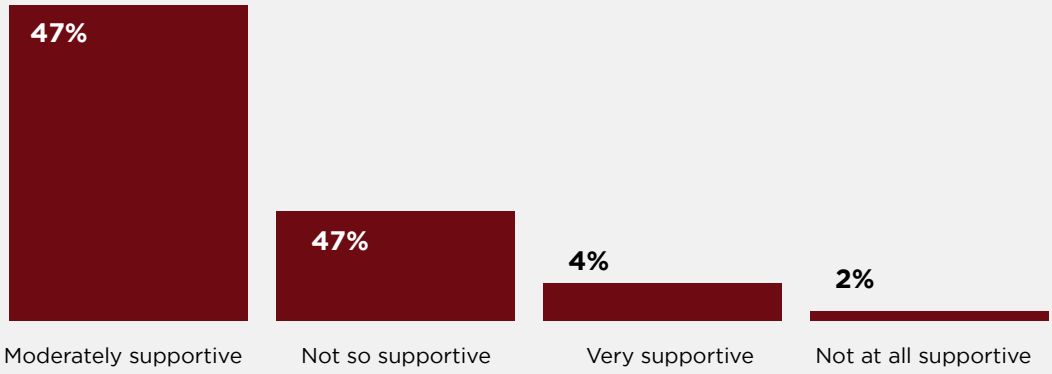
Figure 21: Survey responses on successfully concluded mobile money fraud cases



The United Nations Conference on Trade and Development (UNCTAD) reports that 13% of countries globally do not have cybercrime or related legistation. These countries include Democratic Republic of Congo, Somalia, Central African Republic (CAR), Liberia, Guinea and Bolivia that have mobile money deployments. UNCTAD also indicates that the evolving cybercrime landscape and resulting skills gaps are a significant challenge for law enforcement agencies and prosecutors.[20]

As indicated in the graph below, nearly half (47.06%) of respondents are of the opinion that regulators have been moderately supportive. This suggests that there is some assistance and engagement from regulatory bodies. However, an equal percentage of respondents believe that regulators are not so supportive.

Figure 22: Survey responses on support by regulators



We asked respondents if they pecieved the regulator as unsupportive, and if so, what in their opinion are the reasons why. Their responses can be summarised as follows:

Clarity of mandate: Some respondents feel that combating fraud is not clearly seen as part of the regulator's mandate, coupled with a general lack of understanding of the mobile money ecosystem.

Resources and capacity: There is a consensus that a lack of funding, resources, and technical expertise significantly hinders the regulator's ability to effectively address mobile money fraud. Regulators are perceived by some as ill-equipped to keep pace with the dynamic nature of mobile money fraud.

Legislation and framework: Many cite the absence of effective laws or a robust regulatory framework tailored to mobile money fraud.

Collaboration: A notable lack of collaboration both within regulatory bodies and between regulators and industry stakeholders is identified as a problem.

Regulator's approach: Some responses suggest that when regulators do act, they may focus on punitive measures against mobile money providers in the form of fines, rather than supportive actions that would support providers to address fraud issues.

Adaptability: Regulators are perceived as being unable to adapt to changing times, which is crucial given the rapidly evolving nature of mobile money fraud.

20 UNCTAD. (July 2023). Cybercrime Legislation Worldwide https://unctad.org/page/cybercrime-legislation-worldwide

4.6 Anti-fraud strategies for mobile money fraud

The starting point in managing fraud effectively is developing a robust anti-fraud program that forms a framework for identifying, preventing, detecting, investigating, and responding to mobile money fraud, as described below:

Prevention: This is to prevent, impede and inhibit fraud from taking place. It includes conducting a fraud risk assessment and product diagnostics, developing policies, awareness programs, preventive process and system controls.

Detection: This is the process of monitoring, identifying, and analysing fraud indicators, red flags or anomalies as and when they occur. It includes process reviews and operating detection systems and communication channels that form part of early-warning systems and reporting mechanisms.

Investigation: A standardised robust fraud investigation and response process is important to identify the who, what, when, where and how of a fraud incident.

These should be aligned with an internal control framework that forms three lines: in-business operations, risk and fraud management functions, internal audit.

4.6.1 Fraud prevention

Fraud prevention is a proactive step to prevent, impede and inhibit fraud. The following are the key elements in fraud prevention:

Fraud risk assessment

As indicated earlier, we found that close to half of respondents at 49.02% have not conducted a formal fraud risk assessment. A fraud risk assessment is a specialised form of risk assessment focused specifically on identifying and evaluating the risks of fraud within an organisation. It differs from a general risk assessment in its focus, scope, and methodologies. In particular, it focuses on fraud schemes and how they take place, key risk indicators (KRIs) for that fraud scheme, existing anti-fraud controls in-place, impact and likelihood of the fraud scheme and proposed anti-fraud mitigation measures. A fraud risk assessment must focus on anti-fraud controls and measures.

For instance, a whistleblower hotline is a different reporting channel from a customer complaints channel and while a customer complaints line can be used to report fraud, the whistleblower hotline is specific to fraud, ethics and integrity issues and has certain unique safeguards such as confidentiality, anonymity and non-retaliation. Fraud risk assessments need to be updated continuously to reflect changes in the business environment or operations. New products and processes require formal risk assessment, focusing on loopholes and vulnerabilities that can be exploited for fraudeulent purposes.

Without fraud risk assessments, organisations may not be fully aware of all the potential fraud risks they face, leaving them vulnerable to attacks they have not anticipated or prepared for. In addition, it may lead to ineffective controls as organisations might allocate resources to controls that address minor exposures rather than critical risks, leading to ineffective anti-fraud programs.

Fraud awareness programs

For instance, a whistleblower hotline is a different reporting channel from a customer complaints channel and while a customer complaints line can be used to report fraud, the whistleblower hotline is specific to fraud, ethics and integrity issues and has certain unique safeguards such as confidentiality, anonymity and non-retaliation. Fraud risk assessments need to be updated continuously to reflect changes in the business environment or operations. New products and processes require formal risk assessment, focusing on loopholes and vulnerabilities that can be exploited for fraudeulent purposes.

Without fraud risk assessments, organisations may not be fully aware of all the potential fraud risks they face, leaving them vulnerable to attacks they have not anticipated or prepared for. In addition, it may lead to ineffective controls as organisations might allocate resources to controls that address minor exposures rather than critical risks, leading to ineffective anti-fraud programs.

Case study

Collaborative fraud awareness campaigns in Uganda

Background

Prior to awareness campaigns in Uganda, the country had faced significant challenges with fraud, particularly in the digital and financial sectors. This situation necessitated these awareness and preventive initiatives. The Tonfera Campaign, launched in 2021 by the Uganda Communications Commission (UCC), was an initiative designed to increase public awareness about the safe and responsible use of Information and Communications Technologies (ICTs). The primary aim was to empower consumers to protect themselves from fraud.

The "Beera Steady – Be Better" campaign, launched in March 2023, was an innovative initiative aimed at reducing the prevalence of fraud in Uganda's digital economy. Orchestrated by Next Media and spearheaded by MTN Mobile Money Uganda Ltd, the campaign integrated awareness programs, industry collaborations, and regulatory measures to bolster consumer protection and financial inclusion.
The combination of these two awareness programs synergistically affected anti-fraud efforts in Uganda.

Implementation

The Tonfera Campaign used a multi-channel approach using radio, television, and print media to reach a wide audience across Uganda. It also made extensive use of social media, posting frequent posters to engage with the public. UCC partnered with key players in the telecommunications industry, such as MTN and Airtel Uganda, as well as financial institutions and other stakeholders.

The Beera Steady campaign had a multi pronged approach combining awareness efforts, industry partnerships, and regulatory enhancements to address digital fraud. Significant partners in the campaign included MTN Mobile Money Uganda Ltd, Bank of Uganda (BOU), Uganda Communications Commission (UCC), Financial Intelligence Authority (FIA), NationalInformation Technology Authority of Uganda (NITA-U), Equity Bank Uganda, and the Uganda Bankers Association (UBA).

A key component was educating Ugandans on digital-first business approaches and safeguarding their digital money from fraudsters, thereby promoting financial literacy.

Outcomes

The key outcomes for both campaigns are as follows: Reduction in fraud cases: The campaign achieved notable success in decreasing the incidence of fraud in Uganda. MTN Mobile Money Uganda informed us that mobile money fraud schemes have significantly declined, especially impersonation schemes such as social engineering schemes.

Increased reporting by customers of attempted fraud cases: Customers have increased their reporting of attempted fraud cases as well, with a higher number of cases now being attempts of fraud than actual fraud at a ratio of about 60:40.

Consumer empowerment: The campaign's emphasis on consumer education aimed at empowering individuals with the knowledge and tools necessary to protect themselves from fraudulent activities in the digital space.

Improved collaboration: The campaigns have helped stakeholders and competitors collaborate and come together to fight fraud.

Conclusion

Both campaigns in Uganda stand as a significant effort in combating mobile money fraud through enhancing customer awareness. Their multifaceted approach, involving collaboration across different sectors, use of various media channels, involvement of the regulator and other government agencies demonstrates an effective model for national-level awareness campaigns in the digital age. The campaign's success in raising public awareness underscores the importance of proactive education and cooperation between regulatory bodies, industry players, and the public in the fight against mobile money fraud.

Employee training and awareness

It is critical to conduct regular, internal training sessions specifically aimed at addressing insider fraud. Ethics and integrity programs need to be targeted at creating deterrence and encouraging reporting through whistleblowing channels.

Agent forums

Regular agent forums can be used for ongoing fraud education, focusing on fraud schemes, policies, or changes that have taken place as a result of fraud. They are also a great opportunity for agents to share experiences, challenges, and solutions with the mobile money provider and with each other, helping to foster a collaborative environment. It is also an opportunity to discover issues, trends, and patterns from agents who are regularly in touch with customers and the fraud they encounter.

Background checks and due diligence

This is an important preventive measure for employees, agents and third parties. All employees need to be vetted. Background checks must be made before hiring individuals, especially for positions with access to sensitive financial data or systems. Due diligence should be conducted for all agents and third parties in mobile money before they are onboarded. The first line of defence at agent operations is making sure that all agent documents are in order. The second line of defence is conducting their own independent due diligence checks - this should be risk-based with certain agents and third parties.

Written policies and standards

Employees conducting mobile money activities should clearly understand what is expected of them and their accountablility as dictated by written policies and procedures. There should be no ambiguity in expectations. For example, it should never be the case that in an alleged case of mobile money fraud, there were no daily reconciliations conducted between the bank account and e-money platform without any clear job descriptions and written finance policies mandating the same.

Compliance program for third parties

A majority of survey respondents, 58.82%, reported that sometimes the staff of third-party service providers, such as technology vendors, are involved in fraud, with 21.57% indicating they are often involved. Mobile money service providers need to run robust third-party compliance programs that extend to suppliers - for example, a supplier code of conduct that forms part of the supplier contract.

We found that Safaricom, which runs one of the leading mobile money services, MPESA, has such a program with elements such as partner due diligence and risk assessments, advocacy and multi-sector initiatives, policy requirements (such as supplier code of conduct), monitoring and oversight over third party activities, and communication and awareness.[21]

Preventive process and system-enforced controls

These are important controls in processes and systems to prevent fraud. The following are key controls in this area:

Segregation of duties (SoD): Dividing responsibilities within a process containing multiple individuals to prevent one person from having complete control over key aspects. For instance, separating the roles of authorisation, recording, and reconciliation of financial transactions.

Maker-checker and approvals process: Implementing structured workflows that require multiple levels of approval, with transactions limits that escalate at various levels. Changes in policies, products and services should also go through approval processes.

Regular reconciliation: Conducting periodic reconciliations and comparisons of records, accounts, or inventories to detect discrepancies or irregularities. For instance, reconciling bank statements with accounting records.

Documentation and record-keeping: Establishing clear and comprehensive documentation of processes, procedures, and transactions. This includes maintaining audit trails and logs for actions taken within systems.

Identity proofing solutions: Know your customer (KYC) checks for customers for various identification documents to prevent identity theft or impersonation are important. This includes document verification of official documents provided during onboarding or transactions to ensure their validity. We found that identity proofing solutions such as biometric authentication (fingerprints, facial recognition, or iris scans) are more effective for customer registration and authentication. One of this study's interviewees said that government-driven implementation of biometic registration of SIM cards had reduced their cases of SIM swap and identity fraud in Tanzania by about 90%.

21 Ngige, A. K, CIPE, (2020). Managing Third-Party Corruption Risk: The Case of Safaricom and Its Suppliers: https://www.cipe.org/wp-content/uploads/2020/08/Safaricom-Case-Studies_FINAL.pdf

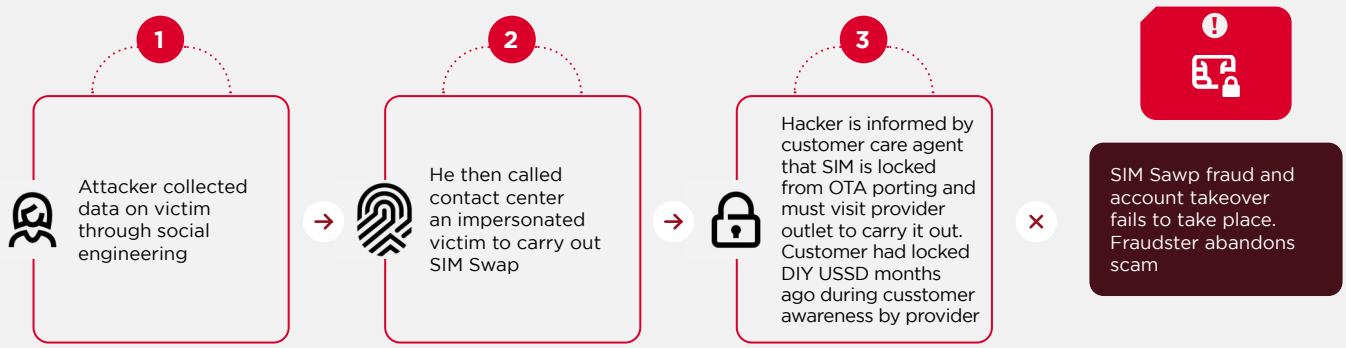
Multi-factor authentication (MFA): This is a control that requires users to provide two or more authentication factors to access an account or complete a transaction. These factors fall into three main categories: something you know (knowledge), something you have (possession), and something you are (inherence). This should be implemented internally to prevent insider fraud and externally at customer touchpoints. For instance, a customer recieves a one-time password (OTP) before completing a transaction. There are other additional controls, such as reducing the timeout of an OTP to prevent its use in case of capture, relay or social engineering. As we were informed in one of our interviews, this was particularly useful for a mobile money provider in Asia.

Strong password management: This is ensuring systems have a strong password policy that includes requiring complex passwords and frequent system-forced password changes.

End-to-end encryption: Encrypting data during transmission to prevent unauthorised access or interception. This will prevent attacks such as man-in-the-middle.

Customer DIY and self-managed controls: Customer do-it-yourself (DIY) and self-managed controls are features integrated into mobile money services that allow users to personally manage their accounts to prevent fraud. These controls empower customers to take charge of their own account security and include various tools and settings that users can customise according to their needs. For instance, a mobile money provider has implemented a customer DIY control that prevents SIM swap fraud by allowing customers to lock the SIM card from any swaps via calls to contact center or agents. After locking the SIM card using a USSD code, the customer can only perform the swap by physically visiting the provider's shop with the nessesary identification documents. Below is a scenario that was shared by one interviewee:

Figure 23: Illustrates a SIM swap and account takeover



4.6.2 Fraud detection

This is the process of monitoring, identifying, and analysing fraud indicators, red flags, anomalies, suspicious patterns or behaviours as and when they occur. These are the key elements in fraud detection measures:

Fraud management system monitoring

Monitoring of transactions helps identify unusual patterns or anomalies. Automated systems flag transactions that deviate from the user's normal behavior or typical transaction size. Monitoring also includes monitoring activity on system access, and agent transaction activity. As indicated earlier, 94.12% of our survey respondents affirm that they have systems in place for managing mobile money fraud. This high percentage indicates that most organisations recognise the importance of such specialised systems in the prevention, detection and investigation of mobile money fraud and have invested in implementing them.

However, the majority of respondents, 54.90% feel that their fraud management systems are not so effective. During interviews, we were informed that many fraud management systems are rule-based systems. Yet mobile money evolves rapidly, and fraudsters continually develop new methods to exploit systems. Some fraud management systems may therefore struggle to keep up with the changes, such a in the example below:

Rule-based system scenario

An 'agent commissions fraud rule' is set in a fraud management system to detect split deposits using number of splits carried out over certain short durations of time at agent tills. This becomes a parameter that fires alerts to a team of fraud analysts. It initially picks several agents and the commissions are clawed back followed by sanctions and penalties on the agent. The agents then notice a pattern of detections based on number of splits they carry out. They then adjust to lower thresholds and longer durations distributed to various tills. The fraud management system suddenly fires less alerts as the rule is ineffective in detecting the adapted behaviour of the perpetrator. Analysts and overseers may misinterpret this to mean that their efforts to deal with commission fraud are effective and may not carry out any further action.

Implementing machine learning algorithms and artificial intelligence enables systems to adapt and learn from new patterns of fraud. These technologies can identify emerging fraud trends and enhance fraud detection accuracy. We found that only 8.33% of respondents use artificial intelligence or machine learning technology in fraud management. The case study below demonstrates how integrating AI in fraud management improves fraud prevention and detection.

Case study

Mobile money provider successfully uses AI to combat mobile money fraud

Introduction

The mobile money sector has experienced exponential growth in recent years, providing convenience and financial inclusivity. However, this growth has run in parallel with the development of highly sophisticated fraud. This case study explains a mobile money provider's strategic deployment of AI and machine learning technologies to enhance fraud detection and prevention in mobile money.

The mobile money provider recognised the necessity to upgrade their fraud detection mechanisms in the wake of increased mobile money transactions. Initially focusing on customer authentication and registration vulnerabilities, they integrated AI to pre-emptively tackle identity fraud schemes and SIM swap frauds. Prior to AI integration, the mobile money provider's fraud prevention rate hovered around 60%. The company aimed to significantly improve upon this and reduce false positives and true negatives.

AI Integration

The organisation implemented the AI and ML algorithms that assign risk scores to transactions based on learned patterns. This model allows the company to predict fraud attempts with high accuracy and adapt to new trends dynamically.

wherever possible, ensuring data is used in real-time. Implementing a continuous feedback loop can also reduce errors and increase true positives.

Outcome

Since the adoption of AI, the mobile money provider has experienced serveral positive outcomes:

- Fraud prevention rate of the specific fraud schemes has increased to around 90%.
- There has been an overall reduction of over 50% in fraud cases.
- Identity theft cases dropped by about 10%, while SIM swap cases saw a decline between 40-45%.
- Agent commission fraud has reduced by over 70%.
- There has also been a significant reduction in false positives and negatives with quick turnaround time (TAT) for the conclusion of mobile money fraud cases.

Conclusion

The mobile money provider journey underscores the transformative impact of AI in fraud management. They have improved fraud prevention and detection rates by continually refining their AI models through feedback loops and using predictive analytics. The mobile money provider continues to push for a 95-97% fraud prevention rate, acknowledging the ever-adapting nature of fraudsters. The company remains committed to enhancing AI capabilities. While AI provides a strong defence against fraud, the company's approach emphasises the importance of continuous evolution and integration of feedback into their systems.

One of the key elements in using AI for fraud detection is integrating and using various data sources and wherever possible, ensuring data is used in real-time. Implementing a continuous feedback loop can also reduce errors and increase true positives.

Detection reviews and audits

Conducting periodic anti-fraud audits and reviews of mobile money systems helps identify vulnerabilities and weaknesses in processes, products and systems. While 88.24% of respondents indicated that they carry out these reviews, 11.27% indicated that they do not. This is essential, especially in reviews and audits focusing specifically on mobile money fraud. These reviews need to be risk-based and focus on high-risk fraud based on a prior mobile money fraud risk assessment.

Process reviews focus on evaluating fraud and irregularities in the procedures and workflows associated with mobile money services. The goal is to ensure that every step of the process is secure and leave no room for fraudulent activities. This includes review and testing of controls such as segregation of duties, maker-checker, authorisation workflows and documentation.

Product reviews are about examining the features and security of products before or after they're launched. These reviews look at how the product is designed and how it can be exploited by fraudsters. They cover product features such as security measures, functionality and interfaces with other products.

System reviews are technical evaluations that focus on the IT software and hardware that supports mobile money service. They are aimed at detecting any technical vulnerabilities that could be exploited. A system review typically involves:

Penetration testing and vulnerability assessments (PTVA): Attempting to exploit vulnerabilities in a system to gain unauthorised access or perform unauthorised transactions.

Infrastructure analysis: Reviewing the hardware and software infrastructure for vulnerabilities, including servers, databases, and network devices.

Access controls and rights management: Evaluating and testing access controls and looking at assigned user rights, who has them, why they have them, and at what level. The review is aimed at ensuring that the principle of least privilege is adhered to. This should include information confidentiality enforcement to ensure information is accessed on a need-to-know, need-to-have basis.

Reviewing multi-layered defence mechanisms: This is reviewing various systems that are part of a multi-layered defence mechanism to ensure they are functioning properly and in concert to prevent fraud, especially insider and cyber fraud schemes. For instance, ensuring a customer relationship management (CRM), data leakage protection (DLP), security information and event management (SIEM) and fraud management system are layered to detect identity theft at the various levels when under attack.

Communication and reporting channels

Customer complaints play a crucial role in detecting mobile money fraud. As indicated earlier, an overwhelming majority (96.08%) of respondents indicated that they detected fraud through customer complaints. A customer is normally the first to notice and report fraudulent activity on their accounts therefore it is important that mobile money providers have established and communicated proper reporting channels to their customers.

Keeping customers informed about recent fraud trends and security updates can also help them stay vigilant. As shown by one mobile money provider in the case study on awareness programs, customers increased their reporting of attempted fraud cases, with a higher number of cases now concluding as attempts only. This feedback from customers helps improve the anomaly detection of internal systems and prevent future incidents.

Whistleblowing programs are an important component - not only for fraud detection but also for corporate governance, compliance and deterrence. They provide a formal mechanism for employees, third parties, and customers to report suspected fraudulent, unethical, illegal, or wrongful behavior. As indicated earlier, a whistleblowing hotline is an anti-fraud control and should have anonymity, confidentiality and protection measures for whistleblowers. Whistleblowing programs are particularly essential in dealing with insider fraud.

4.6.3 Fraud investigation

Mobile money fraud investigations involve a series of steps and procedures aimed at understanding, responding and concluding fraud cases in mobile money financial services. The process is typically complex due to the digital and often cross-jurisdictional nature of mobile money, as presented in this report.

Most mobile money fraud cases, 78%, have a low or very low conclusion rate, as indicated in our survey. This may contribute to an increase in cases since offenders are not being sufficiently dealt with, and this may embolden others due to a lack of deterrence. Conducting proper, timely and thorough internal investigations is important in helping law enforcement authorities and judicial authorities take the next steps.

Information for an investigation to take place can come from the following sources:

- Fraud detection reviews
- Automated fraud detection systems, such as fraud management systems - including those with AI capabilities
- Customer complaints
- Internal audit function
- Whistleblower reports from independent hotline(s)
- Information from staff, agents or third parties during, for example, forums or awareness programs
- Tip-offs or intelligence from regulators, law enforcers or other stakeholders

Investigators should develop a plan outlining the scope of the investigation, the investigation hypothesis, the resources required, the methods used, and the key individuals involved. This plan will serve as a roadmap for the investigation process and ensure its focus. Fraud investigations can be resource-intensive and time-consuming. In mobile money, stolen funds are exfiltrated quickly and therefore there is a need for clarity and speed as well as thoroughness in gathering evidence properly.

Gathering and preservation of evidence

Investigators collect evidence pertinent to a suspected fraud. This includes data and records such as system logs and communication records such as emails, text messages, or call logs. This information should be gathered in line with investigation principles such as legality, chain of custody and preservation of evidence.

Digital forensics is critical in mobile money, and providers are encouraged to acquire digital forensic tools and software for servers, mobile devices, and computers or outsource them to consultants who can do the same.

Forensic laboratories for white-collar crimes, such as mobile money fraud, are important. This is a facility or room designated and equipped for forensic analysis and preservation of evidence. Digital and other forensic tools are housed in this room.
Gathering witnesses and evidence through consultations and interviews is important. Investigators should ensure that this is carried out according to a country's legal requirements.

Reporting, recovery and remediation

Investigators should compile a report detailing their findings, including the methods of fraud, the parties involved, the impact of the fraud, and recommendations for preventing future incidents. One of the key goals is to recover any lost funds. Since customers live precarious financial lives, failure to recover assets or compensate victims when applicable, can seriously undermine customer trust.

A mobile money provider informed us that they created a revolving recovery and refund kitty of $400,000. This is a kitty of funds recovered from fraud cases that is used to refund victims of fraud while legal action is taken to reclaim funds. This fund is also topped up by the provider.

Another key goal is to remediate vulnerabilities that allowed the fraud to occur and by strengthening technical and procedural updates.

$400,000

Amount in a fraud recovery and refund kitty created by a mobile money service provider for customers who fall victim to mobile money fraud

Insurance for mobile money fraud

Mobile money service providers and stakeholders should consider an insurance product that protects customers and providers against financial losses due to fraudulent activity.

Continuous improvement

After the investigation, a review is often conducted to assess the response's effectiveness and improve fraud prevention, detection and investigation measures in future.

An issue and log-management system should be put in place. This can simply be a spreadsheet with columns with categories, such as date reported, fraud scheme/category, issue description, function, perpetrator(s), victim(s), source of information, status, summarised findings, date resolved and comments. All mobile money fraud issues, incidences and problems that are detected, investigated, or reported should be systematically recorded and tracked to maintain accountability and ensure key learnings are not lost. Lessons learned should be ploughed back into the fraud management process. Over time, this information can be used to form a birds-eye view of problematic areas, functions, or processes that allow for risk-based diagnostics and detailed reviews.

05

Conclusion

The rapid growth in transaction volumes and the expansion of operations to accommodate this is likely to increase risk.

The unique characteristics of mobile money, including its accessibility to the unbanked and underbanked, all-round availability, and instant transaction settlements, present distinct challenges in fraud management. The complexity of the ecosystem, involving numerous stakeholders, and the occurrence of multi-stage fraud schemes add to this challenge and require a more multi-faceted and concerted approach.

In classifying mobile money fraud typologies, our research suggests a blended approach to categorisation, incorporating various methods such as attack vector, sector/group categorisation, and others, to capture the multifaceted nature of mobile money fraud. This comprehensive classification is vital for effectively identifying and addressing all potential fraud schemes and sub-schemes. We have further suggested a classification/taxonomy under the main categories of impersonation, insider fraud, cyber fraud and agent fraud. We have also demonstrated that these categories cannot be seen in isolation as there are interconnections at subcategory level and because mobile money fraud involves multiple fraud schemes and types, in what we have called multi-stage fraud schemes.

Mobile money providers have made great efforts to manage fraud. Many of them have a formal mobile money fraud taxonomy, implemented fraud management systems, put in place anti-fraud controls, executed successful awareness campaigns, implemented customer recourse and reporting channels, and put in place remedial measures for customers, including a customer refund kitty for funds lost due to fraud. A vast majority, 96.08%, report mobile money fraud to authorities in attempts to arrest it.

However, they also recognise the increasing and evolving trend of mobile money fraud, and have expressed concerns about the effectiveness of existing systems and approaches. The rapid growth in transaction volumes and the expansion of operations to accommodate this is likely to increase risk. As demonstrated in a case study in this report, the adoption and implementation of more advanced technologies, such as AI and machine learning, can be effective in meeting these challenges.

Effective management of mobile money fraud requires a robust anti-fraud program encompassing detection, prevention, and investigation measures. The absence of formal fraud risk assessments among many organisations presents a vulnerability. Fraud awareness programs need to be expanded for broader outreach and have a cross-industry, multi-sector, collaborative approach. The importance of thorough background checks, written policies, and compliance programs is paramount. For fraud detection, the reliance on traditional systems underscores the need to integrate more advanced technologies. Regular reviews, customer feedback, and effective communication channels, including whistleblowing systems, are crucial for detecting fraud. In terms of investigation, there is a need to make them more efficient through use of advanced technologies, while fostering collaboration with law enforcement authorities. Anti-fraud programs also require continuous improvement so that findings and lessons are ploughed back into the program, making it more effective in future.

06

Recommendations and guidance

Overall, this research emphasises the need for a more sophisticated, multi-layered approach to managing mobile money fraud, involving technological advancement, cross-sector collaboration, and continuous adaptation to the evolving landscape of mobile money fraud. Our key recommendations are as follows:

For mobile money service providers:

Mobile money service providers play a pivotal role in shaping the security landscape of financial transactions in today's digital age. Recommendations are:

- Robust anti-fraud programs: Develop comprehensive anti-fraud programs that include prevention, detection, investigation and response strategies.
- Invest in advanced technology: Use AI and machine learning for improved fraud detection and adapt systems to rapidly evolving fraud schemes.
- Customer education and awareness: Conduct extensive outreach programs to educate customers about risks and preventive measures.
- Enhanced internal controls: Implement strong internal controls, including segregation of duties, maker-checker workflows, multi-factor authentication and identity-proofing solutions
- Third-party oversight programs: Agents, technology providers and other third parties need to be managed in an oversight framework that includes due diligence, risk assessment, regular training, monitoring and enforcement.
- Mobile money providers could explore industry initiatives aimed at facilitating the implementation of trusted partnerships, such as the Mobile Money Certification.

For regulators and law enforcers:

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

- Enhance legal frameworks: Update and enhance legal frameworks to address the specific nuances of mobile money fraud, ensuring laws are robust enough to prosecute such cases effectively.
- Training and capacity building: Provide technical training and resources to deepen understanding and build technical capacity to support players in managing mobile money fraud.
- Collaboration: Bring together various stakeholders to collaborate on various measures, including awareness programs and sharing information.
- Data privacy protection: Enforce clear regulations on the collection, storage, and sharing of user data by mobile money service providers to protect customer privacy and prevent unauthorised access.
- Regular risk assessments: Conduct regular risk assessments of mobile money systems to identify vulnerabilities and implement measures to address specific risks.

The overall aim is to create a multi-faceted and multi-layered approach to combating mobile money fraud. This should involve enhanced regulation, improved technical capacity, comprehensive education and awareness programs, robust technological solutions, and strict ethical standards across all stakeholders.

07

References

GSMA. (2020, March). Mitigating Common Fraud Risks: Best Practices for the Mobile Money Industry. Saad Farooq (Ed.).

Gilman, L., & Joyce, M. Managing the Risk of Fraud in Mobile Money. GSMA.

Raithatha, R., et al. (2023). The State of The Industry Report on Mobile Money. GSMA.

Chalwe-Mulenga, M., Duflos, E., & Coetzee, G. (2022). The Evolution of the Nature and Scale of DFS Consumer Risks: A Review of Evidence.CGAP.

Association of Certified Fraud Examiners (ACFE) (2020). Fraud in the wake of COVID-19: Benchmarking Report

Mudiri, J. L. (n.d.). Fraud in Mobile Financial Services. Hyderabad: MicroSave.

Maina, J. (2023). Cybersecurity: A Governance Framework for Mobile Network Operators. K. Clifford (Ed). GSMA.

GSMA. (April 2023). MMU Spotlight on Direct Deposits https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/04/MMU-Spotlight_Direct-Deposits1.pdf

Clark, J., & Hollinger, R. (2007). Theft by employees. Lexington Books.

Owiti, S. O., Ogara, S., & Rodrigues, A. (2022). A Fraud Management Framework for Mobile Financial Services Within Kenya. The EPRA International Journal of Economics, Business, and Management Studies (EBMS), 9(12).

Outseer. (2021). Outseer Fraud and Payments Report: Digital Transaction Insights from the Outseer Global Data Network, Q2 2021.

Assolini, F., & Tenreiro, A. (2019). Large-scale SIM Swap Fraud. Securelist Research.

Statista. (2020). Volume of Data/Information Created, Captured, Copied, and Consumed Worldwide from 2010 to 2025.

Association of Certified Fraud Examiners (ACFE). (2023). https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud

Mudiri, J. L. (n.d.). Fraud in Mobile Financial Services. Hyderabad: MicroSave.

Safaricom. (2023). Sim swap fraud. https://www.safaricom.co.ke/fraud-awareness/impersonation/sim-swap-fraud

Transparency International. (2023. What Is Corruption? https://www.transparency.org/en/what-is-corruption

GSMA State of the Industry Report (SOTIR) on Mobile Money 2023

Assolini, Fabio, and Andre Tenreiro. 2019. "Large-scale SIM Swap Fraud." Securelist research.

GSMA State of the Industry Report (SOTIR) on Mobile Money 2022

UNCTAD. (July 2023). Cybercrime Legislation Worldwide https://unctad.org/page/cybercrime-legislation-worldwide

Ngige, A. K, CIPE, (2020). Managing Third-Party Corruption Risk: The Case of Safaricom and Its Suppliers: https://www.cipe.org/wp-content/uploads/2020/08/Safaricom-Case-Studies_FINAL.pdf

GSMA Head Office
1 Angel Lane
London EC4R 3AB
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601