

***MicroSave***  
*Market-led solutions for financial services*

## **Fraud in Mobile Financial Services**

**Joseck Luminzu Mudiri**

*A MicroSave Publication*



## Table of Contents

BACKGROUND AND CONTEXT.....	1
KEY ENABLERS OF FRAUD.....	2
MOBILE FINANCIAL SERVICES DEPLOYMENT LIFECYCLE .....	3
CATEGORIES OF FRAUD IN MOBILE FINANCIAL SERVICES .....	8
IMPACT OF FRAUD .....	13
CONCLUSION .....	15
APPENDICES.....	19
APPENDIX 1: CONSUMER DRIVEN FRAUD .....	19
APPENDIX 2: AGENT DRIVEN FRAUD .....	26
APPENDIX 3: BUSINESS PARTNER DRIVEN FRAUD.....	33
APPENDIX 4: SYSTEM ADMINISTRATION AND MANAGEMENT .....	35
APPENDIX 5: MOBILE OPERATOR DRIVEN FRAUD.....	38
APPENDIX 6: DEFINITIONS .....	42
END NOTES.....	44

## BACKGROUND AND CONTEXT

For many years, financial inclusion was a major challenge globally, due to the high costs involved. To offer financial services, premises had to be constructed, new employees recruited and significant capital investments made. Financial institutions concentrated on the high value consumers that yielded larger revenues and largely excluded the majority of the population.

The introduction of mobile telecommunications and later, the adoption of mobile phones to provide financial services changed the dynamics of the industry, bringing financial services closer to the public through existing merchant infrastructure within local communities. The success of M-PESA since its launch in Kenya in 2007 has increased the appetite for mobile financial service deployments especially in developing countries. Financial institutions such as banks and microfinance institutions are also investing in the provision of mobile financial services.

The implementation of mobile financial services, like other financial services, faces risks and challenges. This paper addresses fraud as a challenge in the provision of mobile financial services.

### The Importance of Studying Fraud in Mobile Financial Services

- The study of fraud helps mobile financial service providers build a fraud lifecycle that is closely aligned to the product lifecycle. Different types of fraud will occur at different stages of the product.
- The study will help stakeholders understand the kind of interventions that are necessary to address these risks.
- The study should help lower the cost of intervention by enabling new deployments to learn from older, experienced operators. It is noteworthy that early adopters of mobile financial services learnt from financial services, payments, and telecommunications industries allowing them to mitigate early risks.
- Understanding fraud enables better knowledge of investment required in mobile financial services. Investment costs necessarily include capital investment, infrastructure, platform development, human resources and capacity building to respond to fraud. These costs will be incurred by various stakeholders including regulators, operators, agents and security agencies among others.

### Definition of Fraud in the context of Mobile Financial Services

Fraud is commonly understood as dishonesty calculated for advantage—a deception deliberately practiced in order to secure unfair or unlawful gain. Fraud in the context of mobile money is the intentional and deliberate action undertaken by players in the mobile financial services ecosystem aimed at deriving gain (in cash or e-money), and/or denying other players revenue and/or damaging the reputation of the other stakeholders.

## KEY ENABLERS OF FRAUD

Key fraud enablers in mobile financial services are:

- **Weak regulation** – The inability of regulators to monitor the mobile money ecosystem, to set guidelines for different stakeholders increases the likelihood of fraud in any system. Regulation does not necessarily mean statutory regulation; it may mean oversight by financial regulators. In a number of mobile financial service jurisdictions, regulation is done by oversight with regulators exercising best practice in managing services.
- **Maturity of the mobile money services** - Different types of fraud occur at different stages of the deployment. For example, fraud on B2C and C2B transactions will likely occur in more mature markets, while fake registrations tend to be prevalent in new deployments.
- **Processes** – Weak or non-standardised processes open and enhance the possibilities for fraud. Fraud can be reduced and limited by ensuring that there are checks and balances within systems and structures to limit its occurrence.
- **Compliance monitoring** – Processes alone are, of course, not enough to reduce fraud ... they will only be effective if they are properly monitored. Compliance monitoring will take the form of scheduled audits, independent and mystery shopping, third party reviews, peer reviews etc.
- **Consumer awareness and poor communication within the system** - Communication enables different users to know fraud trends, and mitigants.

Absence of communication may increase fraud occurrence, as new victims will not be aware of the risks and mitigants.

- **High cost of transactions** – When transaction costs are high, customers may try to reduce their costs by abusing the system.
- **Pricing policies** – Pricing and commission paid to different players will contribute to the level of fraud in the system. Percentage pricing has a different impact from staggered pricing and commission. In some cases, the operator may opt to charge for services at a single point and therefore open it up to abuse at points where the service is free.
- **Cultural issues** – Fraud in certain markets will be higher because the society is generally lenient to fraudsters. Leniency may be caused by weak legal structures, or a weak political system.
- **Seasonality** – Fraud tends to increase during certain seasons and activities. As the festive season commences the fraud levels also increase because there are more promotions, and everyone is trying their best to attract funds.

Fraud in mobile financial services mirrors fraud in other financial services such as banking, cards, and ATMs. It is not unique to mobile and therefore lessons learnt in other areas can be replicated in the context of mobile money. Occurrence of fraud depends on the stage of the deployment of financial services. Therefore, the level of incidence will change as the mobile financial service evolves.

## MOBILE FINANCIAL SERVICES DEPLOYMENT LIFECYCLE

A successful deployment will go through three broad stages.

### 1. Customer Acquisition Stage

At this point, the operator wants to acquire as many customers as possible, higher commissions are paid on customer registrations, and agents have one key source of revenue - customer registration commission. The agent value proposition is still unproven and agents spend a lot of time carrying out consumer education. Depending on the market, this stage covers the period from inception of services up to about 2 years of the product. Depending on remuneration of agents, it covers the period when commission earned from registration is more than 50% of total commission paid to agents.

### 2. Transaction Activation Stage

During this stage, customers have been acquired and are being encouraged to transact. This stage revolves around emphasis on the market positioning statement, and driving transactions. Agents earn more commission from transactions and are more loyal to the brand. The operator can reduce registration commissions since agents start earning more from transactions. This stage can take place anytime between 6 months to about the 4th year of the launch of the service.

### 3. Value Addition Stage

The deployment has matured and customers want more. They want to pay for utilities, to transact with their bank accounts, to receive salaries, carry out merchant transactions etc. At this stage the agent channel is important, but cannot handle the nature and volumes of transactions required on its own. Hence the business recruits corporate clients to bring in electronic money. This stage begins at roughly the 3rd year and beyond.

## Fraud Lifecycle Matrix

The occurrence and prevalence of fraud is dependent on the stage of implementation of the deployment. As the deployment evolves, the types of fraud evolve with it. It should be noted that this evolution will depend on the following:

- a) Whether the product focus is also evolving and the deployment is adding different products to the product mix. Some of the newer fraud types will only emerge when new products are introduced. If this does not happen, then there will be little if any change in the types of fraud.
- b) Whether the organisation is identifying, recognising and addressing fraud encountered in earlier stages. If the organisation does not address existing fraud, the type of fraud will persist until the system or deployment collapses under the weight of fraud.



The table below lists prevalent types of fraud and the probability or frequency of its occurrence at different stages of the deployment cycle. This table forms the basic framework of the paper.

<b>1. CONSUMER<sup>i</sup> DRIVEN FRAUD<sup>1</sup></b>	<b>1. Customer Acquisition Stage</b>	<b>2. Transaction Activation Stage</b>	<b>3. Customer Loyalty or Value Addition Stage</b>
<b>A. Consumers Defrauding Agents</b>			
Counterfeit currency	Low	Medium	High
Unauthorised access of agents’ transaction tools	Low	High	Medium
Fraud on agent web channel	Low	Medium	High
<b>B. Consumers Defrauding Consumers</b>			
Phishing, SMS spoofing, fake SMS (Various)	Low	High	High
Extortion	Low	Medium	High
Unauthorised PIN Access	Low	High	Medium
Voucher fraud	Low	High	Medium
Unauthorised repudiation of funds	Low	Medium	High
<b>C. Consumers Defrauding Business Partners</b>			
Impersonation of business organisations	Low	High	High
Erroneous disbursements swindled by recipients	Low	Medium	High

<sup>1</sup>Click on hyperlink to go to Appendix giving details and examples of these frauds and how they might be mitigated

<b>2. <u>AGENT DRIVEN FRAUD</u><sup>2</sup></b>	<b>1. Customer Acquisition Stage</b>	<b>2. Transaction Activation Stage</b>	<b>3. Customer Loyalty or Value Addition Stage</b>
<b>A. Agents Defrauding Consumers</b>			
Unauthorised access to customers’ transaction PINs	Medium	High	Low
Unauthorised use of customer’s transaction code	High	High	Low
Imposition of unauthorised customer charges	High	Medium	Low
Split Withdrawals	Low	Medium	High
<b>B. Agents Defrauding Mobile Financial Service Operators</b>			
Split deposits	Low	High	Medium
Direct deposits	Low	High	High
Parallel money transfer on the network	High	High	High
Registration of customers with fake details	High	Medium	Low
Registration of non-existent consumers	High	High	Low
Registration of individuals as businesses	Low	Medium	High
Money laundering on mobile financial service platform	Low	Medium	Low
<b>C. Agent Employees Defrauding Agents</b>			
Theft of funds	Low	High	High
Underreporting of cash balances	Low	High	High
Copy cat fraud	Low	High	High
Instant Commission Fraud	Low	High	High
<b>D. Fraud By Master Agents</b>			
Unauthorised withdrawals from agent accounts	Low	High	High
Illegal Deductions from Commission earned by agents	Low	High	Low
Illegal sale of agency transaction tools	Low	High	High

<sup>2</sup>click on hyperlink to go to Appendix giving details and examples of these frauds and how they might be mitigated

<b>3. BUSINESS PARTNER DRIVEN FRAUD<sup>3</sup></b>	<b>1. Customer Acquisition Stage</b>	<b>2. Transaction Activation Stage</b>	<b>3. Customer Loyalty or Value Addition Stage</b>
<b>A. Employees of B2C and C2B Organisations Defrauding Businesses</b>			
Employees and fraudsters link wrong mobile numbers to bank accounts	Low	Low	High
Illegal reversal of customer payments to the business	Low	Medium	High
Illegal transfers from business mobile money account	Low	High	Medium
<b>B. Businesses Defrauding Mobile Money Operator</b>			
Settlement fraud	Low	Low	High
Collusion to apply lower tariffs	Low	Low	High

<b>4. SYSTEM ADMINISTRATION FRAUD<sup>3</sup></b>	<b>1. Customer Acquisition Stage</b>	<b>2. Transaction Activation Stage</b>	<b>3. Customer Loyalty or Value Addition Stage</b>
Abuse of passwords	Low	Medium	High
Creation of fake/ non-existent users	Low	High	High
Individual users with multiple rights	Low	High	High
Fraud on multiple access channel (Web and handset)	Low	High	High
Weak Password/Transaction PIN strength	High	High	High

<sup>3</sup>Click on hyperlink to go to Appendix giving details and examples of these frauds and how they might be mitigated

<b>5. MOBILE FINANCIAL SERVICE PROVIDER FRAUD</b> (Click on hyperlink to go to Appendix giving details and examples of these frauds and how they might be mitigated)	<b>1. Customer Acquisition Stage</b>	<b>2. Transaction Activation Stage</b>	<b>3. Customer Loyalty or Value Addition Stage</b>
<b>A. Finance Fraud</b>			
Theft of mobile money provider’s revenue	Low	Medium	High
Issuance of Mobile Money to Organisation against uncleared funds	Low	High	High
Unauthorised access of suspended/dormant accounts	Low	High	High
<b>B. Contact Centre and Operational Support Fraud</b>			
Unauthorised access of customer payment records	Low	High	High
Illegal transfer of funds from customer accounts	Low	High	High
Unauthorised SIM Swaps	Low	High	High
Unauthorised access to co-workers system access rights	Low	High	High
<b>C. Sales and Channel Facing Team</b>			
Bribery	Low	High	High
Fake claims	Low	High	High
Unauthorised access of agent transactional data	Low	High	High
Conniving employees collect deposits from agents	Low	High	High



## CATEGORIES OF FRAUD IN MOBILE FINANCIAL SERVICES

### 1. CONSUMER DRIVEN FRAUD

Consumer driven fraud is fraud that is initiated by fraudsters posing as customers. Consumer fraud targets agents, other consumers, businesses and mobile financial service providers. Consumer driven fraud is the most common fraud in the market and transcends the different stages of the deployment. It is more prevalent during the transaction activation stage of the business when consumers begin to trust the mobile financial service better, but are yet to understand many of the potential risks in the service. The key method of managing consumer driven fraud is consumer education activities, although there are many processes and system-based checks that can also help mitigate these challenges.<sup>4</sup>

The most common types of consumer driven fraud include the following: -

- *Counterfeit (fake) money – Fraudulent customers deposit counterfeit currency with agents and receive electronic money. They immediately withdraw the electronic money at other agent outlets, ATM devices or point of sale devices.*

Mavuno was recently hired by an agent as an employee and part of the mobile money business team. On the second day at his job, a consumer visits the shop. This consumer pretends to know very little about the service but would like to register and deposit some cash. Mavuno, sensing registration revenue, attends to the consumer explaining the service. A second consumer walks into the shop and asks to deposit some funds. Mavuno checks the currency and confirms its authenticity. While Mavuno is confirming the cash, the consumer receives a call and begins to talk on the phone.

He suddenly realises that he has no time and asks Mavuno for his cash, excuses himself and begins to walk out. The first consumer returns to the counter to continue with the conversation. At this point, the second consumer returns, pretending to have changed his mind and requests that Mavuno carries out the transaction urgently. Mavuno obliges and only reconfirms the amount and deposits the cash. He makes the mistake of not checking the currency again and only realises later that the currency is fake.

- *Phishing – Fraudulent consumers send fake SMS to agents either from their own handsets or generated from computers. The SMS looks genuine to the recipient.*

John has been looking for money to pay off his creditors. One day he receives a call from a sweet talking person who claims to represent the largest supermarket chain. The person claims that John has won US\$ 1,200 in a draw that was carried out recently by the company. The caller however has one request, could John send some money (US\$ 100) to account 12345 in order for the winnings to be activated? John obliges and transfers the funds. Next time when John talks to the caller about his winnings, the caller claims that the funds transferred were not enough, and an additional US\$ 100 was required. John borrows the additional funds from his friend Mark promising to repay with interest of 10% per month. After sending the money a second time, he tries to call the recipient but finds his number unavailable. He tries for about 2 hours to no avail. He then decides to contact the mobile operator's call centre. He is duly informed that there is no such promotion going on and several consumers have complained of being defrauded in a similar manner.

<sup>4</sup> Also see Ignacio Mas' [Blog My PIN is 4321](#) for a discussion of these issues.

- *Customers conning agents after creating a relationship with the agent employee – Fraudulent customers develop a relationship with agent employees and con the employees of cash or electronic money.*

Monique is an employee of Zua a leading master agent. Abass is a frequent customer. He always transacts at Zua's shop and tips her every time he transacts. They build a great customer/agent relationship. At some point in their relationship, he calls her and asks her to deposit some money into his mobile money account claiming that he is unable to visit the shop personally. He promises to give her cash in less than one hour. Sure enough, after 45 minutes, he arrives, pays up and tips her. The next week he asks for the same favour and tips her, again. After 3 times of the same behaviour, he strikes. He asks her to deposit US\$ 1,500. This time he disappears, never to be seen or heard from again.



## 2. AGENT DRIVEN FRAUD

Agent driven fraud is perpetuated from within the agent network. The fraud is initiated and operated by agents or their employees. It includes agent employees defrauding agents, master agents defrauding their own sub-agents, agents defrauding customers and, agents defrauding the mobile financial service provider. Agent driven fraud is most prevalent at the beginning of the deployment, catalysed by early loopholes in product pricing. The fraud evolves over time changing form, victims and impact on the deployment.

The key types of agent driven fraud include the following:

### ■ *Employees defrauding agents*

Jampu is a master agent with 20 agent outlets. Bhavesh has been recruited by Jampu as a cash “runner” (someone who gives and takes cash from the shops). Every morning, Bhavesh moves from one shop to another collecting cash where there is excess cash and giving operational cash where there is deficiency. He has always wanted to go to another country and seek better opportunities. He acquires a passport and visa and buys a ticket. One day he takes his route for collecting cash from the shops that have excess cash. He does not return to the office but heads to the airport leaving the country. When the master agent counts his losses, he finds that Bhavesh escaped with more than US\$ 30,000.

### ■ *Split deposits*

Michael would like to deposit US\$ 100 into his account. If he makes this deposit, the agent will earn US\$ 2. In order for the agent to make more money, he splits the money into 10 batches of US\$ 10. Each earns US\$ 0.5 increasing his total commission to US\$ 5 which is much higher than the US\$ 2 should the deposit be done as one lump sum value. Since customers do not pay charges on deposits, they are not worse off with this arrangement.

### ■ *Master agents defrauding agents*

Oblong is an agent network manager and is allowed to recruit sub-agents. Typically, sub-agents should earn 80% of all commissions. However, Oblong understates the total commission earned by the sub-agents by 20%. Instead of paying 80%, he effectively pays 80% of 80% which is 64%. Effectively, the sub-agent receives less commission by  $80\% - 64\% = 16\%$ . This type of fraud affects the credibility of mobile financial service and discourages the sub-agent from further investment in the business.

## 3. BUSINESS PARTNER RELATED FRAUD

Business partner driven fraud describes the fraudulent activities perpetrated from the business partner's network. Business partners include business to consumer (B2C), consumer to business (C2B), and merchants. The fraudulent activities may be perpetrated by employees on the business organisation, employees on customers and partner businesses on the mobile money operator. Business partner related frauds are more prevalent during the value addition stage of the deployment. This is mainly because business partnerships grow at this stage. This type of fraud is still in its early stages because adoption of business transactions is still in its nascent stages.

The most common types of business partner fraud include:

### ■ *Employees of businesses defrauding customers*

Chakitu Bank has recently introduced mobile banking services for its customers. With these services, customers can transact money on handsets. The process involves customers registering for services at Chakitu's branches and Chakitu linking the mobile number to the bank account. Durant, an employee with Chakitu knows a number of customers who maintain large balances in their bank accounts and carry out frequent transactions. They however are not

interested in mobile banking. Durant fraudulently links the customers' bank accounts to his mobile number and transacts funds from their bank accounts to his mobile number. By the time the customers realise they have been defrauded, substantial amounts have been withdrawn.

### ■ *Employees of businesses defrauding the businesses*

Nore Services is a financial institution that has integrated mobile financial services into customer's bank accounts. Customers can transfer funds from the bank account to their mobile money account. Hatari works in the IT department of Nore Services and has taken a lot of interest in these services. Many employees in Nore have little interest in the service and the financial institution has not prepared a proper risk management process document or system to manage risks inherent in the integration. The transactions are not reconciled regularly. Hatari has multiple accesses to the interface that connects Nore to the mobile money service. He takes advantage of this knowledge to transfer funds from the account to several mobile money accounts that he has created over a period of time. When auditors carry out reconciliations after 2 weeks, they discover a loss of over US\$ 100,000.

#### 4. MOBILE FINANCIAL SERVICE PROVIDER FRAUD

This is a range of fraudulent activities perpetrated by the mobile financial service providers' employees. The fraudulent activities will be carried without authorisation of the business. The key types of fraud in this area include fraud on the mobile money operator, mobile money operators' employees defrauding agents, businesses and consumers. Fraud in the ecosystem is less prevalent at the beginning of the deployment and becomes common during the customer activation and value stages of the deployment. At this stage, substantial electronic money has been invested in the system and it therefore becomes attractive to fraudsters.

Examples of the most common types of fraud include the following:

##### ■ *Corruption within the mobile money business*

John is a teacher and is looking an avenue to invest in his spare financial resources. He has recently been told that operating an agency business for a leading mobile financial service provider is lucrative. He decides to try his hand at it and submits the relevant application / documentation. He receives a call advising him that for his business to be given rights to operate the outlet some payment is required as a "facilitation fee". If the bribe is not given, the outlet will not be approved.

##### ■ *Mobile operators' employees stealing funds from the business*

Baku is a leading master agent with 30 outlets and has transacted mobile financial services for over 3 years. Baku is declared insolvent and the business has to undergo liquidation process through the court of law. Baku's mobile money account is frozen pending completion of administration process. Access to the account by the original owners of Baku is cancelled and they can neither view nor transact the account. The liquidation

process takes 5 years to finalise, during which the account is largely forgotten. An employee of the mobile money operator with super-user rights accesses the account and over time transfers funds to himself. By the time the liquidation process is finalised the account has no funds.

##### ■ *Collusion between fraudulent mobile money employees and other fraudsters to carry out unauthorised SIM swaps.*

Jackie is seated in her grocery shop. She decides to make a call to her husband who works in another city. She tries to make her call but is unable to connect. "Another network issue" she mutters and stops trying. She attributes the failure to poor network and continues with her work. Suddenly her neighbour appears extending her phone to Jackie. "It is your husband", she says. She informs her that her husband has been unable to reach her all morning. Jackie realises that she has a problem with her line. When she contacts the mobile operator's call centre using her friend's handset, she is informed that her line has been swapped ... and soon discovers that her mobile money balance has been withdrawn.

##### ■ *Unauthorised access of financial records for personal gain.*

Paul and Michelle are going through a divorce process. Paul suspects that Michelle has more money in her mobile money account than she has declared. He seeks out a customer care employee who agrees to share details at a fee. He pays and he is given the account balance.

##### ■ *Unauthorised transfer of funds from customers' accounts*

John has been depositing funds in his account and transacting quite frequently. He grows suspicious one day when he checks his balance and realises that what he deposited the previous day is missing. He decides to check at the nearest operators' shop and finds that funds have disappeared from his account. He requests for his

statement and realises that a withdrawal of which he has no record or recollection has been made from his account. He lodges a complaint with the mobile money operator specifying that funds have been transferred from his account without his consent. The mobile service provider investigates the transaction and finds that one of the employees accessed the account and transferred funds from John's account into his own personal account. The employee is unable to provide a justification for this action and his service is duly terminated.

## 5. SYSTEM RELATED FRAUD

System related fraud covers all fraud activities that affect the mobile money deployment through system weaknesses and processes. System related fraud will cut across different stakeholders including agents, businesses, and mobile money operators. System related fraud is highest when a platform has inadequate controls to guide in transaction processing. This fraud is prevalent during transaction activation stage of the deployment and continues to grow into the value addition stage.

The key occurrences of fraud include:

### ■ *Password/PIN sharing*

Chantal runs an agent outlet with two employees. Each employee is required to apply for his/her own PIN in order to transact the mobile money business. However, Chantal encourages employees to use the same PIN. Even when employees are terminated from employment, the same PIN is used by newly recruited employees. One day, Mark, one of the employees takes the day off work. He however, passes by the business to check on something and finding the handset lying on the counter, transfers money to a fraudulently registered number. The money is withdrawn at an ATM location. It is very hard to pin the blame on Mark since he should have been off duty on that day.

### ■ *Weak password and transaction PIN strength*

Michi transacts a lot on his mobile banking account. He finds it convenient to do so. His son, Daudi gambles a lot and needs money to feed his habit. Daudi knows his father's year of birth. He has on a previous occasion been instructed by his father to unlock his phone using the year of birth as his PIN. Daudi guesses, correctly, that his father's mobile money PIN is his year of birth. He tries it and is able to send money to himself which he subsequently withdraws.

### ■ *Creation of fake and non-existent users on the mobile financial services platform*

John works for a third party vendor contracted by a leading financial institution. He has been given administrator rights in order to facilitate integration between the mobile money platform and the financial institution. He creates two unauthorised users with rights to initiate and verify transactions, and transfers funds from the organisation to his associates' wallets, effectively stealing money from the financial institution

### ■ *Individual users with multiple rights*

Jim is the Money Transfer Manager with a leading master agent owner. The owner, to save costs, decides not to hire additional staff. He creates himself and Jim as the only persons authorised to transact the main mobile money account. Being a busy man, the owner entrusts his password with Jim, allowing him to act as initiator and verifier on the account. Jim uses this access to transfer funds fraudulently to his friends.

### ■ *Fraud on multiple access channels*

At some point in the business, a leading master agent lost his computer and had to temporarily transact from a computer located inside a cyber café. Subsequently, in an unrelated event, he fires two of his employees Navaro & Sadiki. Even though he now has a new computer he forgets to disable the secure certificate in the cyber café. Navaro & Sadiki being aware, use their access to illegally transact from the cyber cafe.

## IMPACT OF FRAUD

Fraud is not unique to mobile financial services, it occurs in all financial services. Nevertheless, since mobile financial services are one of the high potential methods to increase financial inclusion and extend financial services to the mass market, fraud in this domain has wider implications. Fraud has far reaching impact on the mobile money ecosystem in a number of ways.

### ■ Credibility of the Mobile Financial Service

The credibility of the service will be severely reduced if fraud is rampant and persistent. When employees steal cash from the system, or agents have to pay to access opportunities, the regulator may be forced to intervene in the interests of consumer protection. Individual subscribers will be discouraged from using the services for fear of losing funds through fraudulent activities. The credibility of the mobile money service of a leading Telco in east Africa was severely dented due to a fraud that occurred at the firm.<sup>56</sup>

### ■ Impact on Brand

Brand equity is critical to any business or organisation. An organisation's brand represents the values that define how it is perceived by the environment. If the organisation's products are negatively impacted by fraud, users will associate the brand with fraud and this may also affect any other services or products offered by the organisation.

<sup>5</sup>See Mas and Ng'weno "[Why doesn't every Kenya business have a mobile money account?](#)"

<sup>6</sup> That said, anecdotal evidence from the field suggests that customers' trust was not very badly damaged by the reports of the internal fraud (even though it was large in size) as no customer was affected and only the Telco lost money. Had many agents or end customers been affected, the impact would probably have been much larger.

### ■ Growth in Number of Subscribers

Subscribers want to transact with a financial services platform that is secure, and that they can trust to deliver services promptly and efficiently. In many countries, the fear of fraud and loss of money means that mobile money adoption takes time. In the same way, the adoption of debit and credit cards in developing markets has been negatively affected by fear of fraud. Therefore, if fraud in mobile financial services is not contained, it will affect transaction and customer growth.

### ■ Investment in Mobile Financial Services by Agents

Agents provide critical float and cash to the mobile financial system. This is the key that drives liquidity and therefore the provision of mobile financial services. A high level of fraud in the system will discourage agents from investing in float and cash for fear of loss. Secondly, the agents would be unwilling to commit funds if fraudsters steal funds from their accounts and they are unable to reconcile any commissions earned against what the system shows. Operators are increasingly working with agents to manage fraud within their outlets since it affects their ability to invest in the business.

### ■ Corporate Organisations and Other Providers

The third stage in the evolution of mobile payments is the introduction of Business to Consumer (B2C) and Consumer to Business (C2B) services. Corporate users include banks, utility organisations, salary payment organisations, supermarkets and other organisations that would like to use mobile payments for both receiving and disbursing payments. Due to their volumes of business and thus extensive exposure, they will avoid deployments with a history of fraud that could lead to loss of funds. This therefore limits usage of services at a critical time when the service is growing.<sup>7</sup> A discussion with operators indicates that the process of recruiting banks as C2B and B2C clients is onerous since they have to ensure the security of their funds.

### ■ Innovation and Attitudes

Another negative impact that fraud has is on innovation. Innovation includes opening up the platform to other systems / networks to increase the range of services. Providers will be less willing to take risks and innovate around mobile payments because the entire ecosystem is apprehensive about the frauds that may come with innovation. In order to promote innovation, organisations may be forced to try and limit fraud within the current systems and only subsequently look towards introducing additional services.

### ■ Global Roll Out

Global roll out of the mobile financial services will be negatively impacted by perceptions that mobile payments are prone to fraudulent activities. Perception is critical to adoption of mobile payments deployments globally and therefore as the service becomes fashionable, it is important the successful deployments limit fraud as much as possible. Discussions

<sup>7</sup>See see Mas and Ng'weno "[Why doesn't every Kenya business have a mobile money account?](#)" for an excellent detailed discussion of these and related issues.

with a number of possible deployments have revealed fraud as a key concern, quoting the major losses suffered by the operator in east Africa.

### ■ Cost of Fraud

Fraud and fraud management is a cost that increases overall transaction costs. With high rates of fraud, the transaction charges may have to be raised in order to generate adequate revenue for all stakeholders to sustain the business. If an organisation loses money through theft, or fraudulent activities by third parties, it will be forced to increase charges to sustain the business, making services unaffordable to the broader public. If an agent loses money through fraud, the business may be forced to shut down services.

### ■ Money Laundering

Fraud will, in some cases, lead to money laundering and associated criminal activities. This may include terrorism financing due to lax KYC in customer registration and concealment of funds brought into the financial system by criminals using false identities. Even though there is no evidence so far to show that this is happening, it is important for mobile financial service providers to be aware of the risks around this.



## CONCLUSION

It is evident that mobile money-related fraud is increasingly becoming important. Over the past few years, several serious cases of fraud have been reported that have raised concerns within the industry. As mobile payments begin to scale in many markets and new products are introduced, there is growing need to address fraud conclusively. The donor agencies and consultants have a key role to play in this aspect of the industry.

■ **Research** – There is very limited research into fraud in mobile financial services. This is largely because mobile financial services are fairly new globally with a limited range of successful deployments. Research would involve working closely with these deployments to understand the risks of fraud. In many cases, deployments will be very sensitive about the type of organisation they work with in order to protect their sensitive data. They are therefore more likely to work with independent reputable organisations that are unlikely to compromise on their data. Donors and consultants can play a key role in identifying neutral parties to carry out this research which in the long term benefits the industry. Research will help the market understand the core reasons of fraud, frequency of occurrence, patterns, responsible parties and the effectiveness of various interventions carried out to curtail frauds.

■ **Stakeholder Groups** – As this is a sensitive matter and has a bearing on the brand image and business volumes, many operators prefer to deal with fraud individually without consulting other players. There is therefore limited information flow across parties on similarities in fraud and hence transfer of lessons learned. A fraudster having tricked one financial service provider can move to the next knowing fully well that the information is

unlikely to be shared amongst various mobile money players. Donors and consultants can bridge this gap as neutral parties facilitating such sessions and including other stakeholders including regulators, law enforcement agencies, universities etc.

■ **Development of Smart Tools and Processes** – Smart tools and processes are important in the management of fraud. Most fraud, especially those of a larger scale/magnitude, can be detected and limited through effective data analytics. Many deployments have failed to employ real time, efficient and reliable analytics in mining data. In order to remedy this weakness, deployments may be forced to develop new and better platforms or create interfaces that will enable generation of proper data for mining. Many mobile financial service providers neither have the competence to understand the importance of this activity nor the funds to invest in these activities. They are purely focussed either on scaling up their existing services or trying to develop new products for their customers. Donors and consultants can finance the development of smart tools that can bridge this gap by investing in smart tools and processes on behalf of the providers. They can work with experts to automate services for organisations and identify resources to help in data analytics. They can also design new tool kits should, test them and implement.

■ **Capacity Building** – Many deployments do not have the capacity to understand fraud in their businesses and/or in the industry in general. The body of experts is limited and expansion is yet to keep pace with demand for services. Fields of study previously considered limited in scope are becoming increasingly relevant. For instance there is need for business analysts, fraud managers, money

laundering managers, and compliance officers. It is not the core business of mobile financial service providers to build this capacity. Even if they build capacities in this area, there is a tendency to position experts within their organisations. There is no mechanism to track frauds at an industry level and create faith of the population on the mobile money ecosystem. Donors can bridge this gap by providing funding to create capacity in this field and by helping development of curriculums / training platforms to train different stakeholders in the mobile money eco-system on fraud prevention. Work in this field will have to be an on-going effort which will enable a body of experts to build expertise in this field.

■ **Financial Education** – Financial education is required for both agents and consumers to effectively tackle the menace of fraud in mobile financial services. Financial transactions using the mobile phone are a very recent phenomenon. Even the upper and middle class population—which is better educated and more aware about technology and usage—has not started using the service to its full potential. The low income population, especially the un-banked and under banked, needs to be educated on the usage, benefits and risks among other aspects so that it can confidently use this facility. Similarly, agents will not be able to service the consumers properly and ensure client protection unless they know about the risks and cautions they need to take as service providers. Financial education need not be formal, but involve usage of marketing and promotional tools to drive awareness. There are a number of critical financial education measures that should be considered:

- Agent training and certification – It is widely agreed that agents form the backbone of mobile financial services. Comprehensive training of agents creates the first line of defence against fraud.

Mobile financial services providers must therefore have a comprehensive curriculum in place for initial and on-going training of agents. The curriculum must include certification and evaluation. Well trained agents will be aware of risks, will ensure that customers are made aware of the risks and will know off measures to deal with risks and minimise damage.

- Structured customer and/or agent feedback sessions and events. These forums help to sensitise users and players about mobile financial services and obtain feedback from these stakeholders.
- The use of road shows which focus on experiential interactions between the mobile financial service providers and customers/agents. Road shows have been widely used in the Fast Moving Consumer Goods (FMCG) sector to create awareness around products and services and to address any objections to the products. Mobile financial services are very closely aligned to the FMCG sector and therefore road shows should help providers engage with the customers better.
- Thirdly, adoption of consumer education through awareness campaigns. Awareness campaigns on specific areas of fraud in the print and electronic media will help in sensitising the public about the specific risks.
- **Monitoring and Supervision of Agents**—Investing in channel identification, recruitment and management is critical for successful deployment of mobile financial services. It is costly and requires recruitment of staff, structures, processes and activities that will ensure that the channels or agents provide standardised services to customers. Strong systems and processes are effective only if implemented properly. Regular monitoring of agents is important to check and ensure proper implementation. If there is intentional laxity or

negligence on part of agents, they can be warned; on the other hand if agents make mistakes and are ready to learn, they can be guided through the journey. Periodic audits need to be carried out to verify records and practices, and to hand out performance rewards and (where appropriate) punishment. Mobile financial service providers require the intervention of donors and consultants in providing support and resources to implement these activities. They may need to deploy consultants to help build internal capacity within the organisations.

#### ■ **Mystery Shopping or Compliance Monitoring Activities**–

One of the ways to keep a check on the agents' activities and adherent to defined processes is to conduct mystery shopping. Monitoring and supervision are formal approaches to manage agents' performance and adherence to prescribed processes designed to reduce fraud, but since they are regular and institutionalised, agents often recognise the staff conducting the monitoring/supervision visit. Mystery shopping conducted by people who are not known to the agents can provide invaluable feedback of actual consumer experience. The key drivers of effective mystery shopping include the following:

- Mystery shopping activities should be planned as part of the channel management strategy of the mobile financial service providers. Activities must have well defined objectives and clear monitoring tools. This will ensure that activities are not sporadic but that they are consciously developed by the team. Typically, activities would happen continuously at various levels covering the entire country.
- Mystery shopping activities should be carried out at various levels. The levels include regulators collecting information for their own needs. Regulators are more strategic, looking for “a general feel” of

mobile financial service activities which helps them understand the services better. Activities may also be done by internal management teams and or independent companies contracted to provide independent reviews.

- Stakeholders must be aware of the existence of mystery shopping as a way of quality control. This will ensure that agents work towards ensuring they comply with requirements, demand training from the business if required and provide feedback on quality assessment tools used.
- The rewards and consequences of noncompliance must be defined and communicated to all agents in advance. Agents will therefore be aware of the next steps which will avoid any misunderstanding or fear of victimisation.

■ **Client Protection Reviews**– Client protection measures are those measures that are in place to protect consumers and other users of mobile financial services and therefore the industry itself from unfair practises. A formal review of an organisation's ability to optimise client protection and thus reduce operational, fraud and reputation risk can be carried out through a series of agent, consumer, staff and senior management interviews (and use of other PRA tools).<sup>8</sup> Donors should support these client protection reviews to protect the nascent e/m-banking industry from shocks as recently seen in the microfinance industry. Client protection measures will involve:

---

<sup>8</sup>*MicroSave* has adapted the seven client protection principles developed by Smart campaign for mobile financial services. These are (1) appropriate product offering and delivery, (2) ensuring safety and reliability, (3) transparency of products and services, (4) responsible pricing, (5) fair and respectful treatment of customers, (6) mechanism for complaint resolution and (7) security and privacy of customer data.

- Ensuring effective processes within the business to provide adequate safeguards to users of the organisations mobile financial services. The range of processes put in place by the provider should not compromise client protection at the expense of revenue maximisation and cost savings by the business. Businesses are always trying to maximise revenues and may focus on short term gains which impact client protection negatively. A good example is ensuring that the business implements processes to collect and monitor customer information. This is a costly exercise but it ensures reliable information is always available about users of the mobile money platform. If properly implemented, client protection measures ensure long term sustainability of services.
- The use of industry lobby groups especially association of mobile money providers to set standards that protect consumers. Standards set by an industry association can work to ensure that all providers roll out fair products and take measures that will maintain credibility of services of the industry. Such associations may even work towards uniformity of cross network standards and peer reviews to check compliance to standards agreed to collectively. Such associations may lobby governments on implementation of certain policy actions like counterfeit awareness campaigns to reduce fraud.
- Regulators play a critical role in client protection by defining policy to guide the industry, standards to be followed by mobile financial service providers and regular monitoring of the industry. Regulators of mobile financial services include the financial service regulators, telecommunications regulators, and competitions authorities among others. They must be well equipped to ensure better client protection through promulgation of appropriate policies and the enforcement of policy. Where regulators are not well equipped, they may set poor policy that will in turn impact client protection negatively.



## APPENDICES

### APPENDIX 1: CONSUMER DRIVEN FRAUD

Consumer driven fraud is fraud initiated by fraudsters posing as customers. Consumer driven fraud is the most common type of fraud, targeting many people at the same time. Fraudsters may target agents, other consumers, business organisations and the mobile money operator.

#### a) Consumers Defrauding Agents

TYPE OF FRAUD	EXAMPLE	MITIGANTS
<p>• <b>Counterfeit Currency:</b> Fraudsters mix legal currency notes with counterfeit currency. They deposit money into their wallets at agent outlets. Once deposited, the fraudsters withdraw funds at other agent outlets. Prevalence of such incidents is higher when the deployment is at a transaction activation stage; and secondly, when a new outlet has been opened and staff may have limited experience in identification of legal tender.</p>	<p>Agents with a leading deployment in east Africa have reported cases of 2 or more fraudsters posing as customers distracting them to commit a fraud.</p> <ul style="list-style-type: none"> <li>• The main fraudster pretends to deposit currency at an outlet for electronic money. Once the currency has been confirmed, the fraudster pretends to change his mind and asks for currency to be returned.</li> <li>• The fraudster's accomplice engages the agent employee in mild conversation. At this point, the main fraudster opts to deposit the same currency again.</li> <li>• The agent employee may fail to authenticate the currency, which turns out to be counterfeit.</li> </ul>	<ul style="list-style-type: none"> <li>• Regulators should work with mobile operators to sensitise various channel providers (agents) on security features of legal tender.</li> <li>• Consumer education and sensitisation campaigns on features of legal currency notes. This should include point of sale materials such as posters.</li> <li>• Agents should be encouraged to invest in tools that ease identification of counterfeit currency. Tools include UV lights and currency counting machines.</li> <li>• Provision of hotlines or contact points for reporting fake currency incidences.</li> <li>• Mystery shopping by operators to ensure strict compliance to recommended cash-in and cash-out processes. The key considerations are: <ul style="list-style-type: none"> <li>○ Currency received from consumers must be checked, authenticated and confirmed.</li> <li>○ Customers must confirm that currency they receive from agents is clean before exiting to avoid subsequent disputes on whether the currency is legal or counterfeit.</li> </ul> </li> </ul>

TYPE OF FRAUD	EXAMPLE	MITIGANTS
<p>• <b>Unauthorised Access of agents' Transaction Tools:</b> Fraudsters access the agent's transaction devices (handset/POS device), save their personal details as the mobile financial service provider or as the agent business owner's number.</p> <p>• When the number is saved as mobile phone operator, fraudsters will forward fake withdrawal SMS to the agents who pay assuming they are genuine.</p> <p>• Fraudsters also save their personal numbers as the business owner's number and trick them into sending them money.</p> <p>• Fraud on channels that allow agents to transact on both mobile and web channels.</p>	<p>Reported cases were based on fraudsters (usually known to the employees) gaining access to the trading handset. Some agents observed collusion between some of their employees and the fraudsters especially if the devices are shared by a number of employees. This type of fraud has been reported by many deployments across Africa.</p> <p>Channel providers have reported cases where the business owner asks for funds, and the employee sends money without validating, to a saved mobile phone number in the handset which turns out to be erroneous.</p> <p>A leading operator experienced this type of fraud in central Africa. Agent employees who had prior access to the outlet PIN and password were able to transact on the web and transfer funds from the agent's mobile wallet.</p>	<ul style="list-style-type: none"> <li>• Channel providers should limit access of individuals to their business handset. The handset must be securely stored under lock and key when not in use.</li> <li>• Mobile money operators must disable transaction SIM cards from receiving SMS except from the mobile financial service provider's service. This includes installing filters to block computer generated transactions.</li> <li>• Limit calls to the transaction device to originate from a few pre-authorized numbers of the mobile money operator. These authorised numbers are unique and communicated to channel providers.</li> <li>• Channel providers feedback sessions to discuss fraud and its occurrence.</li> <li>• Limit online transactions to secure terminals with secure web certificates.</li> <li>• To enable online transactions, use a password system that seeks authorisation by the handset or point of sale device.</li> <li>• Transactions carried out on web should send a notification to the handset for record purposes.</li> <li>• Employees of channel providers should not share passwords, neither should they use simple passwords that can be guessed.</li> <li>• Should employees of channel providers be terminated, their passwords should be disabled.</li> <li>• A clear approval process including written authorisation for swapping channel provider's accounts as well as notification of the SIM swap carried out.</li> </ul>

b) Fraudsters Defrauding Consumers

TYPE OF FRAUD	EXAMPLE	MITIGANTS
<p><b>Phishing, SMS spoofing, fake SMS (various):</b></p> <ul style="list-style-type: none"> <li>• Fraudsters send SMS to consumers claiming an ongoing promotion that requires funds to be transferred to the fraudsters' mobile money account numbers.</li> <li>• Fraudsters call a consumer claiming to call from the operator's call centre. The victim is taken through a series of steps which lead to funds being transferred from the customer's account to the fraudster's account.</li> <li>• <b>Extortion:</b> Fraudsters extorting money from consumers and agents through threat of murder/kidnap.</li> <li>• <b>Purported wrong transfer:</b> Fraudsters forward a purported wrong transfer to a consumer. The fraudster follows up with a call to the recipient and claims to have wrongly transferred funds and requests the money back. If customers comply, they will in essence be transferring their own funds to the fraudster.</li> </ul>	<p>The majority of deployments in Asia and Africa have experienced this fraud. It works through phishing. The assumption is that out of a large number of targeted subscribers, some will send money to the fraudster.</p> <p>Most reports of this fraud happen when there is system downtime and customer's transactions affected. This fraud has been reported in many deployments in Africa.</p> <p>This type of fraud has been reported in mature deployments in east Africa and tends to begin with the fraudster gaining as much information as possible from the victim in order to create a false illusion that the consumer is known to the fraudster.</p> <p>This is a type of phishing and has been reported in more mature markets of east Africa. The fraudsters will send a number of fake SMS and follow up with calls. Usually, some of the target victims may transfer funds to the fraudsters.</p>	<ul style="list-style-type: none"> <li>• The mobile financial service provider should minimise the amount of information that is captured on transaction reports at the channel provider's outlet. This information may be misused by fraudsters if they gain access to it.</li> <li>• Consumers must report any threats and fraud occurrences to law enforcement authorities.</li> <li>• For customer facing transactions, it is preferred that such transactions are locked to a handset or point of sale terminal and not online.</li> <li>• Develop an approved SIM swap process and limit the number of people authorised to carry out SIM swaps.</li> <li>• Awareness campaigns to channel providers and consumers on:             <ul style="list-style-type: none"> <li>○ The nature of fraud</li> <li>○ Occurrence of fraud</li> <li>○ Who is at risk?</li> <li>○ How to avoid it?</li> </ul> </li> <li>• Develop clear procedures and guidelines for identification, communication and management of fraud. These procedures include reporting tools and frequency of reporting.</li> <li>• Develop and set guidelines for channel outlets or agents on distance between consumers, privacy of consumers, and specify equipment to limit unauthorised access to customers' transactions.</li> </ul>

TYPE OF FRAUD	EXAMPLE	MITIGANTS
<ul style="list-style-type: none"> <li>• <b>Unauthorised PIN Access:</b> Fraudsters may dupe customers into disclosing their transaction PINs. The fraudsters use the PIN information to defraud the customer once they gain access to the customer’s handset.</li> </ul>	<p>Leading operators carried out extensive PIN campaigns in Kenya, Rwanda and Tanzania sensitizing consumers not to disclose their PINs. Many victims tend to be illiterate and related to the fraudsters.</p>	
<ul style="list-style-type: none"> <li>• <b>Vouchers fraud:</b> Vouchers and transaction codes are generated to enable transfers to unregistered users, ATM withdrawals, online payments, point of sale devices at shops and supermarkets. Vouchers have been in operation for traditional payments services such as western union, moneygram.</li> </ul>	<p>This fraud has been reported by operators at the beginning of the deployment. Consumers steal vouchers from each other and use the same to access funds.</p>	<ul style="list-style-type: none"> <li>• Develop clear processes that define generation of vouchers, expiry periods and notifications on expiry.</li> <li>• Vouchers should not be visible to anyone except the recipient and when misplaced, the recipient can notify the business and get fresh ones re-issued directly.</li> <li>• Preferably, in the case of unregistered customers, they must be required to register before they access their funds.</li> </ul>
<ul style="list-style-type: none"> <li>• <b>Unauthorised Repudiation of Transactions:</b> Fraudsters having received services and paid for them contact the mobile operator and demand reversal of funds to themselves.</li> </ul>	<p>This fraud has been reported in east Africa.<sup>99</sup> In their paper Mas and N’gwenso allude to this fact as the primary reason why businesses don’t use M-PESA.</p>	<p>A clear process to manage repudiation and ensure that the interests of all parties involved are taken care of. A detailed discussion is in the table below.</p>

<sup>99</sup>See Mas and Ng’weno “[Why doesn’t every Kenya business have a mobile money account?](#)”

## Repudiation

Repudiation in mobile financial services means reversal of transactions done between parties (individuals and/or corporate organisations). Repudiation is a controversial subject in mobile financial services as it may lead to intentionally perpetrated fraud.

### Repudiation may involve the following parties:

- Agent depositing funds to the wrong customer
- Customers withdrawing money from agents but keying in the wrong agent identification details
- Customers sending money to the wrong recipients
- Customers sending money to the wrong corporate organisations (C2B)
- Corporate organisations (B2C) transferring money to the wrong customer

### Repudiation of Customer to Business Transfers or Funds Transferred to Agents

Repudiation of such transactions is the easiest because mobile financial service operators maintain contracts that are signed with corporate organisations and agents after detailed vetting process.

- Typically, when money has to be reversed from the agent, the mobile operator will call the agent and confirm that indeed the funds were sent to their account in error. It is highly unusual that an agent will deny the business access to the funds if they were erroneously transferred.
- When funds are erroneously transferred by a customer to a business, the customer may directly inform the business or notify the mobile payments operator who notifies the business. In this case, if funds were not intended for the business, it is also unlikely that they will refuse to reverse the funds.

### Repudiation of Business to Customer Transactions

If funds have been transferred from the agent or corporate customer, the funds can be blocked by the operator urgently and refunded to the organisation immediately they are advised. Affected customers will then be advised of the repudiation.

### Repudiation of Consumer to Consumer Transactions

This repudiation affects transactions from one individual subscriber to another subscriber. It is the most contentious type of repudiation and comprises the largest percentage of transaction repudiations.

There are a number of scenarios in carrying out this repudiation.

#### Scenario 1: - No Repudiation

The operator opts not to interfere with the transactions, callers are advised to either resolve the matter with the recipient directly, or seek legal redress.

#### Advantages

- The operator's resources are not tied to carrying out repudiations
- There is lower risk of repudiation fraud, where the customer obtains services but seeks to defraud the sender by requesting refund of payment.

#### Disadvantages

- The majority of repudiation requests are genuine and genuine customers may lose money
- Customers will rely on goodwill of recipients to refund.
- The recipients of funds will often charge the customers for the refund since there is a cost of transferring the money back to them. This is unlike a reversal which is usually free.
- Consumers may lose trust in the service especially when they have a negative experience and lose funds.

Most deployments have opted not to adopt this approach because it makes the operator appear impersonal.

**Scenario 2: - Call Centre Repudiates Instantly**

The call centre may repudiate transactions on the strength of the sender's request only without consulting the recipient.

**Advantages**

- Repudiation is instant and therefore it will lead to additional transactions on the platform.
- Repudiation is cheaper since no additional calls are required to any other party. Additional calls consume time and resources.
- The requestor's funds are protected before they are misused. There have been cases of consumers receiving funds erroneously and withdrawing the funds instantly.

**Disadvantages**

- There is high risk of repudiating fraudulently requested funds
- Creates mistrust in the system since even fraudulent customers can request for repudiation and funds are credited to their account.
- This option denies the recipient recourse or opportunity to explain his/her position.

**Scenario 3: – Funds are Suspended Prior to Repudiation**

Under this scenario, the customer calls the call centre and requests for repudiation. The call centre immediately suspends the funds to ensure that they cannot be withdrawn. The recipient is then called. If the recipient insists that the funds are genuinely theirs, the call centre employees release the funds to the recipient. However, if recipient accepts that the funds belong to the sender, the funds are reversed and transferred back to the sender.

**Advantages**

- The process is inclusive and both parties have an opportunity to provide feedback. If the recipient surrendered goods and services to the sender this will come out during the call.
- Even when funds are not returned, the sender feels that the operator made every effort to retrieve the funds. Periodic system generated mails to the sender can be helpful. The mobile financial service brand image remains positive.
- The recipient feels obliged to release the funds if they do not belong to him as the call is from the operator.
- It is cheaper for both parties since there is no additional cost to the party refunding

**Disadvantages**

- The recipient may still decline to return the funds.
- The process takes long as both parties must be contacted within a period of time.
- It is costly to the business as the business will have to deploy resources to manage this approach to repudiation.
- The preferred option is scenario 3 since it protects the brand of the company. However additional measures would have to be taken to reduce the incidence of repudiation and therefore fraud. The measures include:
- Enable customers to load numbers they want to transfer funds to directly from the phone address or SIM card into the mobile financial service menu.
- Encourage businesses to register for authorised business services instead of using customer to customer services.
- Add in check digits for business (and possibly consumer) accounts.
- Increased consumer education on repudiation policies.

c) Fraudsters Defrauding Business Partners (Organisations)

FRAUD	OCCURENCE	MITIGANT
<ul style="list-style-type: none"> <li>• <b>Impersonation of business organisations:</b> Fraudsters impersonate as agents of businesses to receive payments from consumers. Fraudsters reach out to the public, providing their personal mobile money accounts and creating the impression that those numbers belong to the organisation.</li>   <li>• <b>Erroneous Disbursements Swindled By Recipients:</b> B2C organisations may erroneously disburse funds to people who choose to withdraw them. Even though the disbursements are initially erroneous (due to employee error), fraud occurs when recipients opt to withdraw the money and close their mobile money wallet.</li> </ul>	<p>A fraudster sets up point of sale (POS) materials (including posters, and signage) in a low income neighbourhood of a major city impersonating as an agent of a leading insurance company in east Africa. The fraudster’s materials solicited insurance premium payments from the public. Prevalence of such frauds is higher in mature markets where adoption rates among businesses for receiving payments via mobile financial services is high.</p> <p>An organisation erroneously transferred more funds than they should have to individuals who participated in a survey. The payments were overstated by overstating the amounts 10 times. Fortunately, the organisation was able to reverse the payments before any of the persons could withdraw the funds.</p>	<ul style="list-style-type: none"> <li>• Develop and publish to the public a clear process for recruitment of corporate organisations with clear KYC requirements.</li>   <li>• Organisations must develop a clear process for disbursement of funds to eliminate errors.</li>   <li>• Comprehensive process that covers identification, monitoring, communication, and management of fraud.</li>   <li>• Enforcement of penalties for channel providers involved in creating businesses as mobile money customers without following the right process.</li>   <li>• There must be a clear customer escalation and feedback process to report fraud cases and trigger market sensitisation of the fraud.</li>   <li>• Businesses must carry out daily reconciliations on payments/receipts against their internal systems.</li> </ul>

**APPENDIX 2: AGENT DRIVEN FRAUD**

**a) Agents Defrauding Consumers**

Agents have the closest contact with subscribers. They play a critical role in registration, cash in and cash out transactions. At the very beginning of the mobile financial service deployment, agents drive consumer education, showing consumers how to use the services and selling the customer value proposition. Subsequently, agents educate consumers on new products and services. Fraudulent agents may abuse their role in the following ways:

FRAUD	OCCURRENCE	MITIGANT
<ul style="list-style-type: none"> <li>• <b>Unauthorised access to customers’ transaction PINs:</b> and subsequent illegal withdrawal of funds from the accounts.</li>   <li>• <b>Unauthorised use of customer’s transaction code:</b> by withdrawing funds from the customer’s account. This happens when new and illiterate customers entrust the agent with the transaction code.</li>   <li>• <b>Split Withdrawals:</b> Agents force customers to split their withdrawals by creating the impression that they do not have adequate cash for the transaction.</li>   <li>• <b>Imposition of illegal consumer charges:</b> Agents can levy charges over and above the recommended customer charges thereby increasing the cost of the service to customers.</li> </ul>	<p>A leading bank in east Africa noticed increased customer complaints on double withdrawals at agent outlets. Investigations revealed that agents would induce customers into carrying out multiple transactions under the pretext that the initial transactions had not been effected. This was done by disabling the POS devices from generating receipts.</p> <p>A new operator in east Africa discovered cases of agents defrauding unregistered customers. Agents would claim that the secret transaction code provided to them by illiterate customers had been unsuccessful and use the same code to withdraw funds at another outlet.</p> <p>This fraud has been reported in Asia and Africa. Agents earning commission under a staggered commission model pretend that they do not have enough cash and request the customer to transact lower values. The <sup>iii</sup>agent earns more commission, while the customer pays a higher transaction charge.</p> <p>Additional charges by agents have been reported in South Asia. Some agents claim charges for transportation, “express processing” etc. In some cases, the customers are aware but have no alternative while in other cases, they may not be aware of the charges.<sup>iv</sup></p>	<ul style="list-style-type: none"> <li>• Develop a comprehensive due diligence process for the recruitment of agents to minimise recruitment of agents with poor reputation or those likely to commit fraud (for example those with a criminal history).</li>   <li>• Document all customer tariffs and communicate through mandatory marketing materials. Channel providers must be required to show customer tariff materials in their shops.</li>   <li>• Carry out periodic and planned consumer and market awareness on PIN security, discouraging PIN sharing. Ensure that relevant campaign documentation is also in all outlets.</li>   <li>• Carry out mystery shopping activities and channel audits.</li>   <li>• Enforcement of legal obligations on channel providers who participate in fraud including termination.</li>   <li>• Involve law enforcement authorities in the management and identification of fraud. Channel providers implicated in fraud should be prosecuted and the acts publicised as a record of commitment of the business to addressing fraud.</li> </ul>

FRAUD	OCCURRENCE	MITIGANT
		<ul style="list-style-type: none"> <li>• Define and enforce electronic money and cash requirements for agents.</li>   <li>• Develop liquidity management tools for agents to monitor their cash and electronic money requirements. The tools may be used by the agent and the mobile money operator to track daily, weekly or monthly requirements. They may also set limits based on seasonality, activities, and specific activities that would affect requirements.</li>   <li>• Automation of all customer tariffs and agent commissions either on the mobile money platform or on the client organisation's platform.</li> </ul>

**b) Agents Defrauding Mobile Money Operators**

The relationship between agents and mobile money operators is mutually beneficial. Agents earn commission on transactions while operators extend their services to a wider public, conveniently and faster. Agents may take advantage of loopholes in the mobile money platform and processes to earn more revenue from the system. Instances of fraud in this regard include the following:

FRAUD	OCCURENCE	MITIGANT
<ul style="list-style-type: none"> <li>• <b>Split Deposits</b><sup>10</sup> are carried out when an agent encourages customers to split cash in transaction values into smaller tranches in order for the agent to make additional revenue. Split deposits are more prevalent on staggered commission model and flat rate commission model. There is motivation to split commission in a percentage commission model.</li> <li>• <b>Direct Deposits:</b> MNO driven deployments require customers<sup>v</sup> to deposit into their mobile wallets (free of charge) and to transfer the funds at a small cost. Agents may encourage customers to bypass the transfer charge by depositing directly into the recipients account.</li> <li>• <b>Parallel money transfer on the network:</b> Agents may facilitate money transfer transactions off the mobile financial service through agent to agent transactions which are usually free to the agents.</li> </ul>	<p>A number of leading operators in east Africa experienced high levels of split deposits that increased their cost base. The channel providers were able to earn higher commissions and therefore adversely affect the profitability of the service. The operators addressed the situation through generation of reports that track split deposits, significantly improving their revenue flows.</p> <p>An operator in southern Africa is experiencing challenges with direct deposits since customers prefer to deposit directly into recipients accounts to avoid paying transfer fees. The operator’s customer charge includes the transfer fees and withdrawal charges.</p> <p>Some agents in southern Africa and south Asia have established a parallel money transfer system, sending money to other agents and giving details to customers to withdraw the funds. The impact of this transaction is that the agent and customer benefit while the operator is denied revenue.</p>	<ul style="list-style-type: none"> <li>• Document legal obligations of agents with regard to split deposits and enforce appropriate redress on those found conducting split deposits.</li> <li>• Carry out consumer education campaigns to create awareness about these types of fraud including the use of merchandising materials, posters and fliers.</li> <li>• Analyse and review agent commission structures regularly to detect any anomalies and address them. Preferably, commission must be reviewed half yearly.</li> <li>• Carry out mystery shopping activities at agent locations to detect incidence of split deposits, direct deposits and compliance to KYC requirements.</li> <li>• Develop smart systems that can identify direct deposits using the GSM network. GSM can identify deposits carried out by a channel provider in one location and credited to an account in another location.</li> <li>• Regulators must set guidelines on compliance requirements and reporting. The mobile money operators must report periodically on the key compliance standards.</li> </ul>

<sup>10</sup> See *MicroSave* India Focus Note 71 “[Sustainability of BC Network Managers \(BCNMs\) in India - How are BCNMs Paid?](#)”

FRAUD	OCCURENCE	MITIGANT
<ul style="list-style-type: none"> <li>• <b>Registration of customers with fake or non-existent KYC documentation:</b> Such registrations may be carried out by fraudulent agents to earn commission as well as to facilitate fraud by registered customers.</li> <li>• <b>Registration of non-existent consumers:</b> by registering customer lines yet to be sold to consumers. Agents carry out such registration to earn commission.</li> <li>• <b>Registration of individual subscribers in the name of businesses</b> in order to receive payments from the public.</li> <li>• <b>Money Laundering:</b> Misuse of relationship with mobile money operator as a conduit for money laundering or other criminal activities.</li> </ul>	<p>Many operators in west and east Africa are going through a clean-up exercise after determining some of the records were inaccurate. Agents in east Africa have been terminated by operators for wilful fraudulent customer registrations.</p> <p>There have been reported cases in Asia of registration of consumers not interested in the business with the agent sharing the commission with the customers. This leads to high levels of dormant accounts.</p> <p>In east Africa, mobile operators experienced cases of agents registering consumers as businesses. This registration fraud usually occurs in cases of collusion between agents and fraudsters. Careless agents may be unwittingly misled to register fraudsters as businesses in contravention of KYC rules.</p> <p>This fraud remains unreported but it is highly likely that agents may use their relationship with mobile money operators to launder money or create a false positive impression about their activities.</p>	<ul style="list-style-type: none"> <li>• Regulators must use their authority to enforce standards among mobile money operators. They may suspend the operator’s licence, cancel the licence, and compel the operators to act in a more proactive manner.</li> <li>• Regulators must listen to the public and provide feedback to operators to address challenges that affect registration.</li> <li>• Regulators and mobile money operators should carry out subscriber registration of customers on the mobile network and link this to mobile money registration.</li> <li>• Mobile money operators should work closely with national registration authorities, the primary authorities that issue identification to validate identification documents.</li> <li>• An approved process for consumer recruitment covering required customer documentation and preparation of training guides for all channel providers.</li> <li>• Customer registration commission to be split between registration and transaction.</li> <li>• Charge agents for any illegal commission collected from the business.</li> </ul>

**c) Agent Employees Defrauding Agents**

Agents are on the frontline of mobile financial services. They are motivated by income that they generate from registration, cash in and cash out transactions. Agents recruit employees to carry out these transactions. This presents a different set of fraud challenges that they must deal with on a day to day basis. High levels of fraud by employees may affect the agent’s business viability and therefore willingness and/or ability to invest in the business.

FRAUD	Occurrence	MITIGANT
<ul style="list-style-type: none"> <li>• <b>Theft of agent’s funds</b> by employees. Agent employees may steal their employers’ funds. The employees may resign, abscond or continue working until they are discovered by their employers.</li> <li>• <b>Underreporting of cash balances:</b> Systematic underreporting of cash balances by agent employees. The underreported difference is invested by the employees in their own businesses or activities. In some cases, the employees will collude with employees of other agents and during inspection by business owners, temporarily advance credit to each other to cover variances.</li> <li>• <b>Copycat fraud:</b> Agent employees may take advantage of a surge in certain types of fraud and purport to be victims of such fraud. The employees divert the “lost” funds to their own use.</li> </ul>	<p>An agent in central Africa closed one of his outlets permanently because the employee in the outlet absconded with the entire cash and electronic money investment. The business owner is hesitant to open more outlets until he is able to manage the risk.</p> <p>An agent with a leading operator in east Africa reported noticing that electronic money in one of his outlets was trading on average below 50% of his investment. On investigation, the employee denied any differences. The business owner organised a surprise audit, arriving at the shop before commencement of the day’s operations. He reconciled the account and the employee could not account for 50% of the investment. The employee had diverted funds into her personal business. She was promptly arrested and she refunded the money.<sup>vi</sup></p> <p>A number of agents suspect that when there is an upsurge in certain types of fraud, some of their employees participate in the fraudulent activities and pretend to be victims of fraudsters. This cannot be discounted because this type of fraud also happens in other financial services and retail businesses.</p>	<ul style="list-style-type: none"> <li>• Channel providers should carry out adequate background checks of potential employees before recruitment to ensure that they are seen as being trustworthy and do not have undeclared criminal history.</li> <li>• Channel providers must enforce a two-step approval process for all their web transactions to ensure accountability. One employee initiates transactions, while a second employee verifies.</li> <li>• Channel providers should carry out frequent and <i>ad hoc</i> audits of their outlets to ensure that they have adequate float and cash.</li> <li>• Channel providers must ensure that all outlets balance their float and cash on a daily basis before they close business and report any variances.</li> <li>• The mobile money operator should avail reports on the platform to enable channel providers to manage their businesses.</li> <li>• The mobile money operators should create forums that enable channel providers to exchange ideas on various issues and best practice in tackling fraud.</li> <li>• The mobile financial service providers should work with channel providers to identify affordable</li> </ul>

FRAUD	Occurrence	MITIGANT
<p>• <b>Instant Commission Fraud:</b> For commission models that pay instant commission, business owners find it difficult to reconcile commissions earned as they become mixed up with other transactions. Employees take advantage of this mix up to defraud their employers.</p>	<p>In west Africa, agents of a leading deployment found it difficult to reconcile commissions earned from transactions because the commissions were paid instantaneously into their business wallet. The deployment is considering accruing and paying commission at the end of the month</p>	<p>fidelity insurance cover to cover them against theft by servant, and robbery.</p> <ul style="list-style-type: none"> <li>• Creation of a database of blacklisted agent employees to monitor fraudulent employees.</li> <li>• Involvement of law enforcement authorities in investigation of fraud.</li> <li>• Aggregation of commission payments to agents for payment after a scheduled period of time preferably monthly. A report should be generated specifying commission earned, the mode of payment and any reference number for the payment.</li> </ul>

**d) Fraud By Master Agents**

Master agents are appointed by mobile financial service providers to manage agent outlets set up under their networks. They are critical in providing first level support to agents and facilitate faster roll out on behalf of the operator. Master agents need to have a high level of integrity as they can negatively impact confidence of stakeholders in the business. The most common fraud types by master agents include the following:

FRAUD	OCCURENCE	MITIGANT
<ul style="list-style-type: none"> <li>• <b>Un-authorized withdrawals from agents’ accounts:</b> Master agents carry out unauthorised withdrawal of funds from sub-agent’s accounts. This denies sub-agents of their money and any incomes that may accrue to them from transactions.</li>   <li>• <b>Illegal Deductions from Commission earned by agents.</b> This may occur through illegal charges by master agents such as overstatement of any taxes, as well as understatement of commissions earned by the sub-agents.</li>   <li>• <b>Illegal sale of agency tools.</b><sup>vii</sup> Master agents are allocated agent tools to operate agent outlets, which they resell to outlets instead of activating them.</li> </ul>	<p>A number of outlets in one of the east African deployments reported complaints about agents withdrawing electronic money from sub-agents accounts without authorisation in the early days of the service. This operator placed limitations on master agent access to sub-agent accounts which has eliminated this fraud.</p> <p>This fraud has been reported in Africa and Asia. Sub-agents are supposed to be paid a specific percentage of all commissions. Some master agents only pass on a percentage of the total commission due, retaining the balance for themselves, thus reducing the commission available for the sub-agent. This type of fraud affects the credibility of the mobile money provider and discourages the sub-agents from further investment in the business.</p> <p>There have been reports in a number of deployments in east Africa about this type of fraud. Affected deployments counter the fraud by terminating contracts of companies involved.</p>	<ul style="list-style-type: none"> <li>• A clear agent recruitment process defining the role of master agents and sub-agents.</li>   <li>• Detailed contracts and guidelines for operation of master agents regarding obligations, staffing and requirements for sub-agent recruitment.</li>   <li>• Approved operational guidelines defining clear consequences of poor management of sub-agents and the process to be followed to remedy the consequences, if any.</li>   <li>• Implement guidelines on commission sharing between master agents and sub-agents and provide these on the mobile money platform so as to ensure uniformity across channels.</li>   <li>• Facilitate sub-agents to carry out transactions independent of master agents. Limiting the master agent’s role to relationship management, and report provision.</li>   <li>• Facilitate direct crediting of the share of sub-agent’s commission directly to the sub-agent’s account and the need for master agent’s to receive and disburse the sub-agent’s share.</li>   <li>• Independent audit of sub-agents and document findings on performance of their master agents.</li>   <li>• Provide sub-agents with adequate feedback forums including hotlines, email addresses, and sub-agent forums to receive feedback.</li> </ul>

**APPENDIX 3: BUSINESS PARTNER DRIVEN FRAUD**

**a) Employees of C2B and B2C organisations Defrauding Organisations**

As the mobile money deployment grows, the operator extends services to meet evolving customer needs. The new services introduce different types of fraud. Employees of partner businesses may take advantage of loopholes in the process, mobile money platforms and controls to defraud the business. Due to the sensitivity of fraud among businesses, fraud occurrence is rarely, if ever reported. Typical fraud types include the following:

FRAUD	OCCURENCE	MITIGANT
<ul style="list-style-type: none"> <li>• <b>Employees and fraudsters link wrong mobile numbers to bank accounts:</b> Collusion between employees and fraudsters to link fraudsters’ mobile numbers to the customers’ bank accounts facilitating withdrawal of funds from the bank account.</li> <li>• <b>Illegal reversal of customer payments to the business:</b> Illegal reversal of funds from the mobile money account of the business by employees even when services have been rendered to the paying party. The employee will collude with the paying party and benefit from this reversal.</li> <li>• <b>Illegal transfers from business mobile money accounts:</b> Illegal transfers by employees responsible for payments from the corporate organisations mobile money accounts. This may include transfers to the wrong recipients, creation of fake disbursements, among others.</li> </ul>	<p>As part of facilitating bank withdrawals into mobile money accounts, an employee with a leading bank in east Africa fraudulently linked a customer’s bank account to his mobile number. He could withdraw funds from the customer’s account using his own PIN number. The employee was quickly discovered and terminated.</p> <p>This type of fraud is yet to be reported or publicised. It is however more likely to happen if the organisation maintains weak controls in payment and reversal processes.</p> <p>This type of fraud has not been reported or publicised. This fraud would typically happen if there is collusion between employees and fraudsters to create fake users and disburse funds to them.</p>	<ul style="list-style-type: none"> <li>• Corporate clients should reconcile all mobile money transactions, addressing variances on a daily basis.</li> <li>• Organisations should maintain separate accounts for receipts and disbursements to limit the exposure of the client to fraud.</li> <li>• Withdrawals from the client organisation’s mobile money account must follow a two-step process with separate approvers and verifiers.</li> <li>• For customers linking their bank account to the mobile money account, the corporate should ensure that:                         <ul style="list-style-type: none"> <li>○ Customers complete a form with the bank and signs appropriately allowing the account to be linked.</li> <li>○ A responsible officer with the bank counter checks the details with the customer through alternative methods such as calling the customer or paying him a visit.</li> </ul> </li> <li>• The bank must send a notification message to the real owner of the bank account to which the link is made.</li> <li>• Banks must set a limit to the transactions that can be done on a daily basis on a customers’ mobile money account.</li> <li>• Organisations should limit the number of people who can initiate changes to a customer’s bank account link to a mobile number.</li> <li>• The organisation must maintain a log of persons carrying out any changes on the mobile banking platform.</li> </ul>

**b) B2C AND C2B Organisations Defrauding Mobile Operators**

Business partners may defraud the mobile operator of revenues earned from transactions. The most likely source of fraud is through collusion with employees as described below.

FRAUD	OCCURENCE	MITIGANT
<ul style="list-style-type: none"> <li>• Collusion of mobile operators’ employees with customers, business partners’ and/or agents to apply lower tariffs fraudulently.</li>   <li>• <b>Fraud on settlement of charges:</b><sup>viii</sup> Business partners (consumer to business) clients are required to settle charges on transactions before they withdraw funds due to them from the operator’s account. If the platform allows it, businesses can withdraw the entire payment without settling any charges owed to the mobile financial service provider.</li> </ul>	<p>This fraud is more likely to happen on business facing transactions. In such cases, employees of the operator may have greater flexibility in applying different tariff<sup>ix</sup> regimes for organisations.</p> <p>Mobile operators in east Africa have reported cases of corporate partners inadvertently not settling charges when they withdraw their funds. The risk will become bigger as more organisations are recruited to receive and disburse funds.</p>	<ul style="list-style-type: none"> <li>• Documentation of tariff and commission implementation processes with clear guidelines on tariff policy, affected parties, business rules and implementation periods.</li>   <li>• Documentation of a clear technical implementation and testing process of approved tariffs and commission separate from the approval process.</li>   <li>• Separation of the roles of persons who set business rules, customer tariffs and agent commissions on the platform, and the roles of people who administer the platform.</li>   <li>• Regular and <i>ad hoc</i> audit of the tariff and commission implementation process and technical settings is critical.</li>   <li>• Automate settlement of customer to business (C2B) charges before funds are withdrawn or paid to the business. When a corporate recipient of funds withdraws money from the system, the charges must be debited automatically and a statement made available on the system.</li> </ul>

**APPENDIX 4: SYSTEM ADMINISTRATION AND MANAGEMENT**

Mobile financial services credibility requires accuracy and fast turnaround time of transactions. Because mobile financial services are technologically driven, the technology introduces a different set of risks. The risk of fraud is in system administration, password management and misuse of access rights. The table below describes the most common types of fraud and how they should be mitigated.

FRAUD	OCCURENCE	MITIGANT <sup>x</sup>
<ul style="list-style-type: none"> <li>• <b>Abuse of passwords</b> on the mobile money platform by different users including super administrators, super users, administrators, and other staff.</li>   <li>• <b>Creation of fake and non-existent users</b> on the mobile money web platform. These users will initiate and approve transactions on the platform and handsets moving electronic money from agents or corporate organisations mobile money accounts – thus reducing the operator’s ability to track the source of fraud.</li>   <li>• <b>Individual users with multiple rights:</b> Users with rights to initiate and verify transactions can defraud the organisation that has entrusted them with such access rights.</li> </ul>	<p>This fraud is yet to be publicly acknowledged.<sup>xii</sup> An example of incidence would be during creation of users by the administrator. The administrator accesses the password of the user yet there is no prompt to the user to change it. The administrator misuses this access to make changes on a customer’s transaction account.</p> <p>This type of fraud is yet to be reported. It happens in situations of weak controls on the mobile financial services platform.</p> <p>This type of fraud has been reported by master agents in operations in east Africa. This fraud will occur when the owners of the business maintain very weak controls in the business.</p>	<p><b>Super-Administrators’ Rights</b></p> <ul style="list-style-type: none"> <li>• Clear separation of roles on the system between super administrators, administrators, super-users and users. Super administrators’ roles should be limited to creation/deletion of administrators and super-users. Administrators should be limited to creation/deletion of users, while users should be limited to carrying out transactions.</li>   <li>• Super administrators must be approved and set up with the approval of the highest possible authority in the mobile financial services provider. All relevant documentation must be filed.</li>   <li>• The creation/deletion of administrators must have at least a two-step approach.                             <ul style="list-style-type: none"> <li>✓ Documented request from an authorised person on behalf of the organisation through approved process.</li> <li>✓ Implementation of the requested changes on the platform by the super-administrator.</li> </ul> </li>   <li>• Automation of password generation on the mobile money system that is invisible to other users. All users must be required to change their passwords when they log into the system for the very first time.</li>   <li>• All creation and deletion of users must be carried out on a secure terminal (computer) with secure certificates. Audit of the process must be carried out frequently.</li> </ul>

FRAUD	OCCURENCE	MITIGANT <sup>x</sup>
<p>• <b>Fraud on multiple access channel (Web and handset):</b> Platforms that can be accessed from remote locations such as cyber café can be misused by fraudsters with access information to such accounts. It is also well known that fraudsters are able to install software on public computers that can read passwords. In some cases, fraudsters may read details on SIM cards and clone the SIM cards as is prevalent in the card industry.</p> <p>• <b>Weak password/transaction PIN<sup>xi</sup></b> strength on mobile financial service platforms. Weak passwords can be discovered by fraudsters through trial and error. Passwords prone to such abuse include 4 digit transaction PINs. Many consumers use their year of birth.</p>	<p>Employees will use their superior access to steal money and provide fake reconciliation reports to the owners.</p> <p>A leading operator in central Africa detected fraud which involved fraudsters accessing the web to transfer money from the mobile money account of agents.</p> <p>There have been frequent reports of customers of leading mobile money providers in Africa being defrauded by their relatives because the relatives can correctly guess their PINs.</p>	<p><b>Administrators</b></p> <ul style="list-style-type: none"> <li>• Administrators should be created or deleted by the super-administrator on the strength of an authorisation letter from the user business/department.</li> <li>• Administrators should be limited to creation and deletion of other users and not operational tasks.</li> <li>• A system generated summary of users created by administrators should be forwarded to the highest authority in the organization for notification.</li> <li>• Preferably, new users should only become operational after 24 hours of being created and subsequent confirmation by the highest responsible authority in the organisation/department.</li> </ul> <p><b>Users</b></p> <ul style="list-style-type: none"> <li>• Develop clear processes for all types of transactions.</li> <li>• Set transaction limits for different types of users. For simple customer facing transactions such as cash in/cash out, users can transact without the need for approval of the transactions.</li> <li>• For more complex and web facing transactions, there must be a two-step process: <ul style="list-style-type: none"> <li>○ One user to initiate transaction</li> <li>○ A second user verifies.</li> </ul> </li> <li>• Users should never be able to initiate and verify the same transaction.</li> <li>• A transaction log must be maintained detailing any requests made on the platform and the party that carried out the request on the platform.</li> </ul>

FRAUD	OCCURENCE	MITIGANT <sup>x</sup>
		<p><b>Password/PIN Management</b></p> <ul style="list-style-type: none"> <li>• Passwords/PINs should never be shared by users, super-users, administrators, super-administrators.</li> <li>• Preferably, passwords/PINs should not be visible to parties other than the users. If not, the users must be required to change password on first log in.</li> <li>• Complexity of passwords/PINs. Preferably, ensure that pins have more than 4 characters to limit users from using their year of birth as password/PIN.</li> <li>• All terminals (devices) that carry out web transactions must operate under a security certificate and must be regularly audited.</li> <li>• All security certificates must automatically expire within a specified period typically no longer than one year and fresh certificates must be granted after this period.</li> <li>• In the event of an employee’s name being deleted from the list, the certificate that he is using must be cancelled and a fresh one issued to anyone joining is his/her place.</li> <li>• The mobile money system should keep track of all certificates issued to various teams and preferably, shared with the organisations periodically.</li> <li>• Every organisation must maintain a fraud management team. The team must carry out fraud sensitisation activities with all users including agents, business partners and mobile money providers’ employees.</li> </ul>

**APPENDIX 5: MOBILE OPERATOR DRIVEN FRAUD**

This may be referred to as “Fraud in the family”. This type of fraud is perpetuated by employees of the mobile financial service provider on the business, its partners and other parties. Fraud in the family affects the credibility of the services and is usually a reflection of process failure.

**a) Finance Administration Fraud**

Mobile money creation process begins when organisations deposit funds into a bank account that mirrors mobile money account. Funds in the bank account must equal total funds in the mobile money ecosystem. The ecosystem comprises consumers, agents, corporate businesses, and various revenue accounts of the operator. These funds are vulnerable to various risks that may affect the credibility of the product. They include the following:

FRAUD	OCCURRENCE	MITIGANT
<ul style="list-style-type: none"> <li>• <b>Unauthorised finance staff access C2B, B2C or agent’s main mobile money accounts</b> and transfer mobile money float deposits made into these accounts to other account holders.</li> <li>• <b>Theft of mobile money provider’s revenue.</b> Internal employees defraud the mobile money operator, targeting sale of airtime, customer charges, funds that may be unclaimed, dormant accounts and other revenue streams. The funds may be diverted to fictitious accounts and withdrawn from the mobile money system.</li> <li>• <b>Issuance of mobile money to organisations against uncleared funds.</b> Staff responsible for issuing electronic money can do so on the strength uncleared funds such as cheques,</li> </ul>	<p>This type of fraud is yet to be reported. It is likely to happen in a system that has poor processes for deposit and for transfer of float.</p> <p>A deployment in east Africa almost lost money through an employee who attempted to withdraw funds from the organisation but was thwarted in time to stop the transaction due to effective controls.</p> <p>MTN Uganda, part of a leading global telecommunications company, reported in the media the loss of over USHS 9 Billion (US\$ 4 Million) in fraud by employees. According to the company, this fraud was perpetuated by employees who were able to access the company’s funds after an upgrade.<sup>xiii</sup></p> <p>This fraud would occur if an organisation deposits a cheque into a trust account. The amount should only be credited when the funds clear. However, in the event of collusion between</p>	<ul style="list-style-type: none"> <li>• Reconciliation of float and cash in the bank must be carried out daily and signed off by a responsible official of the business.</li> <li>• Mobile money accounts for businesses and agents must be set up only after the organisation has been approved, with a valid contractual relationship.</li> <li>• The businesses (agents/corporates) must complete details with accurate information of contacts and banking details and sign off these details.</li> <li>• Any changes to the mobile money agents/business account holders’ details must be properly authorised by a responsible party within the requesting organisation.</li> <li>• All revenue reporting lines, and airtime accounts must be reconciled on a daily basis to track cash in, cash out and balances.</li> <li>• Suspense accounts should be checked and balanced on a daily basis. Any suspense accounts should only have balances current to 24 hours.</li> <li>• Develop clear processes for external parties to deposit money into the bank for float, verification of deposit and resolution of disputes on deposits with clear service level standards.</li> <li>• Preferably, all withdrawal requests of funds from the mobile money partners</li> </ul>

FRAUD	OCCURRENCE	MITIGANT
<p>telegraphic transfers, and other methods before the amounts are actually credited to the partner organisation’s account.</p> <ul style="list-style-type: none"> <li>• <b>Unauthorised access to channel providers’/ organisations’ suspended accounts.</b> If these accounts remain suspended for long periods of time, they may be accessed and the funds withdrawn.</li> </ul>	<p>employees and the depositors, funds may be credited in advance. Such incidences are yet to be publicly reported in mobile financial services.</p> <p>This fraud is yet to be reported. However, as deployments evolve, the possibility of employees abusing dormant accounts will increase if the deployment maintains weak controls.</p>	<p>should be automated and managed by authorised employees and not manually. The employee logs onto the web interface and carries out the transaction instead of writing a letter to the mobile money operator to do so.</p> <ul style="list-style-type: none"> <li>• In the absence of web access, all withdrawal requests must be on headed paper and signed by an authorised person within the organisation.</li> <li>• The Finance team should only process withdrawals upon confirmation that the request is valid and comes from the correct person.</li> <li>• The withdrawal of funds should be approved by at least 3 independent parties within the mobile financial service, i.e. 2 people who check the system to make sure that the request is valid, and the last two who approve funds to be debited from the bank account.</li> <li>• Before payment of funds to any partner’s account, the authorised person in the partner organisation should be contacted to confirm the withdrawal by a responsible person within the mobile financial service provider’s team.</li> <li>• All relevant documentation including transaction logs of the withdrawal must be maintained and audited regularly.</li> <li>• The organisation must define circumstances and periods of dormancy<sup>xiv</sup> on both business and customer accounts. At no time should any of the accounts that hold substantial amounts of money be allowed to stay dormant for longer than the set period. Dormant accounts should be flagged, frozen and account holders contacted</li> <li>• Any revenues arising from vouchers generated should be audited and reconciled regularly even if the vouchers remain unutilised.</li> </ul>

**b) Contact Centre/Customer Care Teams**

Contact centre employees are the first line of call for consumers and other stakeholders that contact the business. To facilitate their work, they will be granted access to contact centre sites, and can carry out certain actions such as making changes on customers’ accounts. This role presents different types of fraud that must be addressed by the business.

FRAUD	OCCURENCE	MITIGANT
<p><b>Unauthorised<sup>xv</sup> access of call records for personal gain.</b> Customer care teams have access to customer records and can misuse this access to sell customer transaction information to third parties or share the information to fraudsters.</p>	<p>This fraud is yet to be reported by providers. Typical fraud will happen when a fraudulent employee provides transaction details to fraudsters to facilitate extortion or phishing.</p>	<ul style="list-style-type: none"> <li>• The mobile money provider should maintain a CRM for handling consumer challenges. The system must include the following                             <ul style="list-style-type: none"> <li>○ Type of issue</li> <li>○ How long would such an issue take to resolve.</li> </ul> </li> </ul>
<p><b>Unauthorised transfer of funds from customers’ accounts</b> to other people’s accounts. Employees with access will use tools available to them to move funds.</p>	<p>This fraud is yet to be publicly acknowledged by any provider. It is very likely to happen when customer accounts are dormant over long periods of time.</p>	<ul style="list-style-type: none"> <li>• The business must maintain a customer escalation procedure to handle all complaints from customers and manage resolution.</li> <li>• Contact centre teams must be vetted before they join the business.</li> </ul>
<p><b>Unauthorised SIM swaps<sup>xvi</sup></b> occur when a customer’s SIM card is swapped without authorisation for a new SIM. The holder of the new SIM card can access the mobile money account and transact. The SIM swaps may be intentionally carried out by employees of the mobile financial service provider or the employees may be led to swap after fraudsters pass the vetting process.</p>	<p>An operator in central Africa fired employees for this fraud, while a second operator in East Africa arraigned an employee in court.</p>	<ul style="list-style-type: none"> <li>• Maintenance and review of transaction logs on the platform tracking all access to the system and accounts with special time stamps and reference numbers.</li> <li>• Customer care roles should be limited to reversal of transactions and not movement of funds from the account to other accounts. This should be escalated to another team either within customer care or outside customer care.</li> </ul>
<p><b>Unauthorised access to co-workers access rights on the system.</b> The fraudsters find a way to access the log in details and misuse this access on the mobile money platform.</p>	<p>Some employees in mobile financial service deployments may share passwords or maintain easy to guess and thus abuse passwords. This type of fraud is yet to be publicly acknowledged. However, it happens in the financial sector and therefore may happen in mobile financial services as well.</p>	<ul style="list-style-type: none"> <li>• Document a clear SIM swap process which limits people/organisations that can carry out SIM swaps and establishing time limits between the time that SIM swap is carried out and the time it is implemented.</li> <li>• Keep track of swaps carried out through reports.</li> </ul>

**c) Fraud Caused by Corruption of the Sales Team**

It is globally acknowledged that the key to success of mobile financial services is the management of distribution structures. The frontline sales team is responsible for identifying, recruiting and managing agents. This unique position may be abused by the team for purposes of personal financial gain. The types of fraud include the following:

FRAUD	occurrence	MITIGANT
<ul style="list-style-type: none"> <li>• <b>Bribery.</b><sup>xvii</sup> Employees may demand cash for favours such as approval of agency applications, processing of corporate transaction accounts, etc.</li> <li>• <b>Fake claims.</b> Managing channel providers requires significant field travel by the distribution team. Some of the team may provide fake claims for travel expenses.</li> <li>• <b>Unauthorised access of agents’ personal information.</b> Employees may demand access to agents’ physical records and tools and carry out changes on the account in collusion with fraudsters.</li> <li>• <b>Conniving employees may take deposits from agents</b> with the pretence of depositing the funds on their behalf.</li> </ul>	<p>Corruption is more likely to happen in mature markets. In east Africa, a number of employees have been fired as a result of engaging in this type of corrupt activities.</p> <p>Fake travel claims affect not just the mobile financial services sector, but many other sectors too. Without proper controls, they can result in substantial losses to the business.</p> <p>Even though unreported, agents have sometimes complained of persons masquerading as employees of the operator gaining access to their records and linking this to frauds that happens later.</p> <p>A leading bank in east Africa terminated an employee for collecting deposits from an agent and not remitting them to the agent’s account.</p>	<ul style="list-style-type: none"> <li>• Develop and document a clear process for channel recruitment and management. The process must cover the following:                             <ul style="list-style-type: none"> <li>○ Required criteria</li> <li>○ Approval timelines and milestones</li> <li>○ Dispute resolution</li> </ul> </li> <li>• Automate the recruitment process and communicate to the public via necessary channels for information.</li> <li>• Set up clear communication channels for applicants to report and provide feedback on gaps and corruption in the approval process.</li> <li>• Automate entire application and management process to ensure that issues are flagged when they occur.</li> <li>• Clearly define and document the relationships between performance of the channel providers and provision of additional outlets or additional tools of trade.</li> <li>• All channel recruitments must be approved with a proper checklist and sign-offs.</li> <li>• Maintain a database or tracking list of tools of trade including SIM cards to be issued to outlets, any recovered, suspensions and balance in the market. An audit should be carried out of these tools.</li> <li>• Maintain a separate sign-off of all tools sent to channel providers and set up on the mobile money system.</li> <li>• Review of reports of all outlets approved for agents against applications/performance and qualification standards.</li> </ul>

## APPENDIX 6: DEFINITIONS

■ **Agent** – An agent is an outlet, shop, premises, channel where mobile money transactions can be carried out on behalf of the mobile money providers. Agents are registration, cash in and cash out points for customers. Agents earn commissions on transactions and act on behalf of the mobile financial service operator.

■ **Business to Business transactions** – These are transactions between businesses. A business may transfer funds to another business. These transactions are not very common in mobile financial services. As merchant services are introduced, such transactions will begin to pick up.

■ **Business to Customer (B2C) transactions** – Also known as Business to Consumer transactions, these are transfers initiated by businesses directly to subscribers. They may be government social payments, salary disbursements, loan disbursements or any other transfers initiated by organisations directly to individuals.

■ **Customer to Customer (C2C) transactions** – Also known as Consumer to Consumer, Peer to Peer, Person to Person, these are transfers between one individual mobile money subscriber and another individual subscriber.

■ **Customer to Business (C2B) transactions** – Also known as Consumer to Business transactions, these are customers transferring money to business organisations. The transfers include merchant payments, utility payments, insurance premiums, bank deposits, or any other customer initiated transfers to organisations.

■ **Flat commission**–Flat commission structure is one where an organisation or agent receives a flat amount for transactions irrespective of the value. This commission is common in the banking sector. Usually, this structure does not adequately compensate high value transactions and may therefore encourage agents to split transactions.

■ **Flat customer tariffs**–Flat customer tariffs are tariffs set that do not change with transaction value. These charges are popular in the banking system and are sometimes applied by banks carrying out branchless banking. In mobile financial services, they are common in peer to peer transactions that do not attract additional costs to the operator.

■ **Know Your Customer (KYC)** – KYC is a term for a range of requirements mandated by regulators or operators to facilitate transactions within the network. The objective of these requirements is to ensure that to the best possible extent, a customer or organisation is identified before they are allowed to transact within the ecosystem. Usually KYC is required by regulators, although some operators may opt to ask for additional requirements. KYC includes identification for transactions, completion of a transaction document and signing of a document to confirm that a transaction has been completed.

■ **Master Agent** - Also called Super Agent, Agent Network Manager or Aggregator. A Master Agent is an organisation that owns or manages a number of agent outlets. A Master Agent is usually appointed by the mobile financial service provider.

- **Mystery shopping** – A discrete process of observation by stakeholders to test whether transacting organisations or agents are complying with required processes.

- **Percentage commission**–Percentage commissions are commissions paid to agents as a percent of the transaction value. The percentage commission structure discourages low value transactions that may earn negligible commission but encourage agents to carry out high value transactions since the compensation is evenly spread.

- **Percentage customer tariffs**–Percentage based customer charges borrow heavily from the card business where merchants are charged a percentage of the transaction. Customer charges are levied as a percentage of the value transacted. Percentage customer charges are common in west Africa, southern Africa and Asia for peer to peer transactions. In east Africa, percentage tariffs are levied on utility payments and merchant transactions.

- **Staggered commission** – Commission paid to agents based on value bands. The commission will only change when the customer's transaction value moves to the next value band. The key benefit of this commission structure is that for lower value transactions, the agent is guaranteed a minimum commission which allows the agent to carry out low value transactions.

- **Staggered customer tariffs** – Staggered customer tariffs are flat charges on customer transactions set for different value bands. The charges change only when a customer transaction value moves to the next value band. These charges are popular in mobile financial services and borrow heavily from the Western Union model. These charges are common in east Africa and central Africa.

- **Super administrators** – Super administrators are the persons who hold the main password and access to the platform. If these users does not exists the entire platform will not function.

- **Administrators** – Administrators are created by super administrators. Their role is to manage system functionalities at different levels such as creation of users, end of day processes, system back up, and general maintenance.

- **Super users** – A super user role is an operational role that has the most superior rights of manipulating transactions on the mobile financial services platform. The super user can manage all modules on the platform except the administration and set up modules. Usually the super user approves different rights granted to other users.

- **Users** – Users are created by administrators. Their role is to manipulate transactions on the system within certain modules. Users are usually approved by super-users and their rights are dependent on approval by the super users.

## END NOTES

<sup>i</sup>For purposes of this document, consumers are individuals who are either existing customers of the service or not. Fraudulent activities carried out by consumers are similar whether the consumer is registered or not. In many cases, a consumer intent on committing fraud, may register for the service just to defraud other participants in the mobile money ecosystem. In other cases, a consumer may be lured into registering for the mobile money service by a fraudulent customer to enable the consumer transfer funds to the fraudster.

<sup>ii</sup>Regulators protect customer information through privacy laws. This makes unauthorised access to customer data a criminal offense. Employees may be motivated by financial gain in accessing customer data even though it could lead to criminal prosecution.

<sup>iii</sup>Under staggered tariffs, agent commission as percentage of customer transaction value is higher on lower transaction values as compared to commission earned on higher transaction values. Therefore, an agent is likely to earn more commission by splitting a single withdrawal into more than one transaction than processing the withdrawal in a single transaction.

<sup>iv</sup>When a leading global telecommunication provider launched its mobile financial services in Africa, customer charges were not set on the mobile payments platform. Under this tariff, customers would pay for services charges directly to the agent in cash. This translated to multiple charges in the market due to lack of coins and change. Effectively, Agents earned more commission than was recommended by the business. Customer confidence in the deployment was damaged and the operator was forced to discontinue the practice. Subsequently, all customer charges and agent commission were set on the system.

<sup>v</sup>Many deployments do not charge for deposits in order to encourage cash into the mobile financial system. Once the money is put into the system, operators earn revenues from follow up transactions such as transfers, withdrawals, airtime purchase among others.

<sup>vi</sup>We have also seen that in east Africa, agents prefer female employees to male employees. There is a perception that male employees have a higher incidence of fraud than female employees.

<sup>vii</sup>Agents need SIM cards and point of sale devices to carry out transactions. Obtaining these tools is essentially obtaining a license to provide mobile financial services. Some Master Agents may obtain these tools and resell to others.

<sup>viii</sup>In customer to business transactions (C2B), operators allow the business to settle charges levied for services against receipts only when the C2B organizations want to access their funds. Employees of the organisations will therefore confirm the total receipts against what is owed to the mobile financial service deployment periodically. Once this is done, they should deduct the charges owed from total receipts. Many platforms do not automatically deduct charges and therefore organisations can still settle without deducting charges due to the mobile financial service provider.

<sup>ix</sup>In most business facing transactions, mobile financial service providers set different tariffs for different businesses. In some cases, each individual organisation will have its own tariff. This happens mostly when the operator has few business partners in place. In a number of deployments, operators set different sets of tariffs for different types of business. Some businesses will attract lower tariffs because of projected high volumes or a special relationship with the operator. In both cases the deployment will have a process of implementing the tariffs approved for the businesses. There is a risk that processes in place may be weak and therefore abused by employees.

<sup>x</sup>[The Observer - How MTN lost mobile billions](#) by Jezz Mbanga, dated 24th May 2012. The exact nature of this fraud is not clear. Press reports point to unauthorised access of employees to customer accounts. The operator claims that employees stole money directly from the company and customers' accounts were not affected. Whichever version is correct, this fraud points to weak controls in the business leading to the loss of a substantial sum of money.

<sup>xi</sup>The risk presented by dormant accounts is quite big especially as the deployment matures. In banking, there is a very clear definition of dormancy, and dormant accounts are very closely monitored. In mobile financial services, dormancy on subscribers is dependent on regulation set for telecommunications providers on SIM cards before they are recycled. In many cases, this is usually 6 months. Many operators are yet to define dormancy

on businesses partners or agents whose mobile money accounts may not be dependent on SIM cards recycling processes. This is clearly risky to the business and operators should define dormancy for businesses, and set clear process for managing such accounts.

<sup>xii</sup>Regulators protect customer information through privacy laws. This makes unauthorised access to customer data a criminal offense. Employees may be motivated by financial gain in accessing customer data even though it could lead to criminal prosecution.

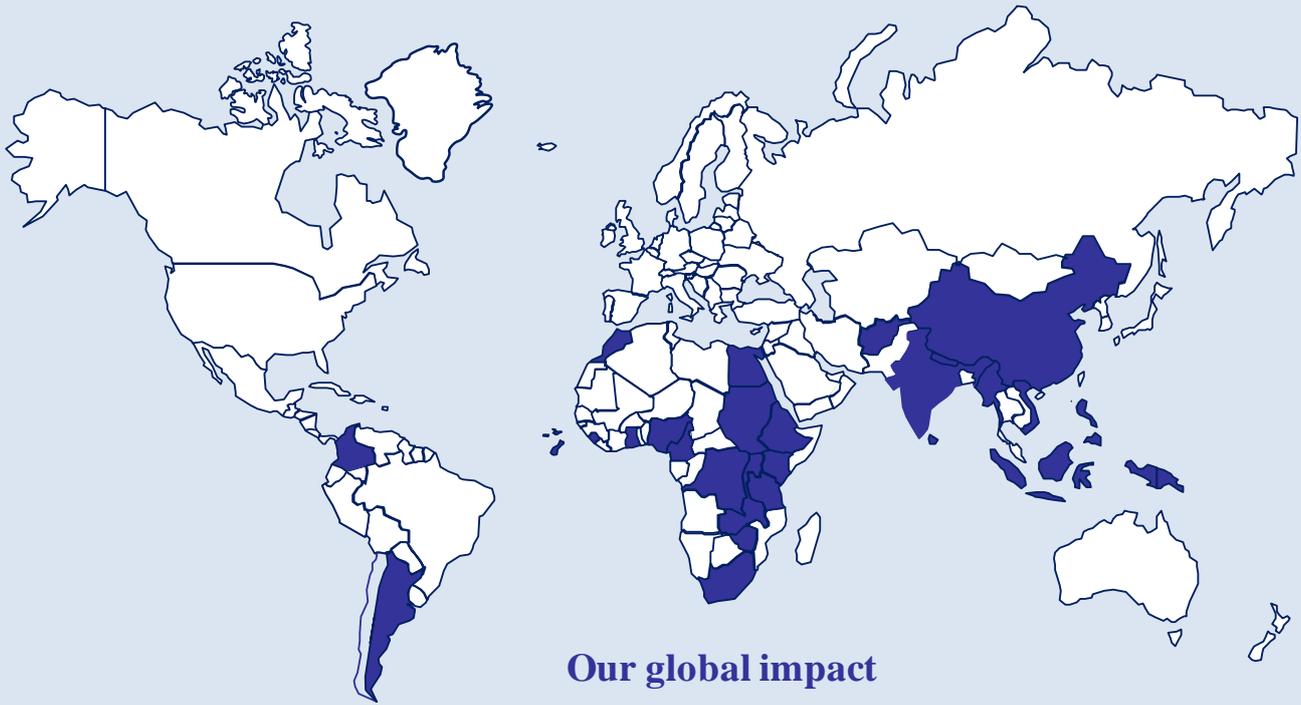
<sup>xiii</sup>[MTN Moves To Prevent Sim Card Swap Fraud In South Africa](#): This SIM swap was carried out erroneously but resulted in loss of funds to a charity in South Africa.

<sup>xiv</sup><http://www.itwebafrica.com/telecommunications/153-kenya/229957>. In this article that appeared on 11th September 2012, the Safaricom CEO acknowledges firing 16 employees for bribery. Bribery becomes prevalent when mobile financial services are perceived as lucrative business with few barriers to entry by potential investors.

<sup>xv</sup>Some mobile payment platforms are very flexible. They allow the mobile financial service provider to set risk management structures on the platform based on need. This may be counterproductive since the operator may intentionally set weak processes that result in fraud. In the event of fraud, the platform provider's image will also be dented. It is important for platform providers to set a minimum risk management structure on the platform to guide operators. For example all platforms must have an initiator, verifier relationship for all web facing transactions.

<sup>xvi</sup><http://finance.yahoo.com/blogs/the-exchange/cracking-pin-code-easy-1-2-3-4-130143629.html>. In this blog Nick Berry, founder of [Data Genetics](#), a Seattle technology consultancy has found that many people use very simple characters and numbers for PINs and passwords. They include years of birth, 1234, 1111, and easy iterations of 1313 etc. This shows that there is considerable chance of fraudsters correctly guessing PINs.

<sup>xvii</sup>It is very difficult for operators and business partners to publicly acknowledge password management fraud in any financial setting. This would be acknowledging that their processes are weak.



## Our global impact

### MicroSave offices worldwide

**INDIA**   
 Head Office: Lucknow  
 Tel: +91-522-2335734  
 Fax: +91-522-4063773  
 New Delhi Office:  
 Tel: +91-011-45108373  
 Hyderabad Office:  
 Tel: +91- 40-23386140  
[info@MicroSave.net](mailto:info@MicroSave.net)

**ARGENTINA**   
 Saavedra 1086 Apt C.  
 Ciudad Autónoma de  
 Buenos Aires, (1229)  
 Argentina.  
 Tel: +54-9-11-6965-778

**INDONESIA**   
 Jl. Penjernihan I No. 10,  
 Komplek Keuangan -  
 Pejompongan,  
 Jakarta Pusat 10210,  
 Indonesia.  
 Tel: +62 82122 565594

**KENYA**   
 Shelter Afrique House,  
 Mamlaka Road,  
 P.O. Box 76436, Yaya 00508,  
 Nairobi, Kenya.  
 Tel: +254-20-2724801/2724806  
 Fax: +254-20-2720133  
 Mobile: +254-0733-713380

**PAPUA NEW GUINEA**   
 First Floor,  
 Town Post Office,  
 Port Moresby  
 Papua New Guinea  
 Ph: +675-3434789

**THE PHILIPPINES**   
 Unit 402, Manila Luxury  
 Condominiums,  
 Pearl Drive corner Gold Loop,  
 Ortigas Center, Pasig City,  
 Metro Manila, Philippines.  
 Tel: +(632) 477-5740  
 Mobile: +63-917-597-7789

**UGANDA**   
 Regency Apartments  
 30 Lugogo By-Pass  
 P.O. Box 25803  
 Kampala, Uganda.  
 Tel. +256 312 260 225  
 Mobile. +256 776 36 5536