# Risk management in Mobile Money:

## Observed Risks and Proposed Mitigants for Mobile Money Operators

**Andrew James Lake**

**November 2013**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
**State Secretariat for Economic Affairs SECO**

IFC International Finance Corporation
World Bank Group

# Contents

## Introduction

Mobile Financial Services offer significant opportunities for improving the efficiency of financial services by expanding access and lowering transaction costs. The rapid public acceptance of these services in many countries, including the Philippines, Brazil, India, Uganda and Kenya has demonstrated that the technology is mature and brings real benefits to people who previously could not access financial products or services.

IFC has recognized the potential of using Mobile Money as a mechanism to deliver financial inclusion and, in November 2012 Mobile Money was formally adopted as a significant part of its Access to Finance work.

According to the GSMA[1] website, as of September 2013, there are 192 live Mobile Money operations in the world, and a further 109 in planning. In 2012, the GSM Mobile Money survey[2] indicated that there are 82 mil people registered for Mobile money globally. With this number of operations and a growing number of customers involved in the service, formalized risk management which balances the assurance of an enabling environment that is conducive to innovation and economic development against consumer protection concerns becomes more and more important.

This importance is amplified in Annexures A and B to this document, which highlight emerging fraud trends in Uganda. In one case, a supplier of Mobile Money services lost $3.5 million to a single type of fraud. The inherent nature of the frauds observed in Uganda is not reliant on any specific aspect of Uganda's economy or social structure and is thus replicable in many other Mobile Money operations if processes are not put into place to control the risks.

## Products currently being sold within Mobile Money operations

Across the 192 live deployments, Mobile Money and / or the Agency Banking model which it enables have been applied to:

- Deposit and transact products
- Over the counter bill payments
- Intra country remittances, both over the counter and based upon the Mobile Transaction accounts
- International remittances
- Savings products
- Lending products (Secured and unsecured)

[1] The GSMA is the global industry body representing nearly 800 of the world's mobile network operators.
[2] http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/02/MMU_State_of_industry.pdf

Selling and servicing each of the products above via Mobile and Agency banking introduces a set of risks, some of which are common across the product lines and some of which are unique to each product.

## Mobile Financial Services Model Definitions

1. **Bank Model**: In a pure bank model a bank (or other licensed deposit taking institution) holds the customer funds. Each client either holds an account with the bank, or a Mobile Wallet. The service typically provides mobile access to balance inquiry, transfers between accounts, and payments. Access can be provided through the Internet or through a cell phone based system where a cell phone menu is used to guide the customer. The bank assumes responsibility for the service.

   This type of service provides convenience to existing bank clients and to the bank itself by enabling some routine transactions to be performed without visiting a bank branch, which saves time and costs for both the client and for the bank while enabling bank branches to serve a larger number of clients due to the reduced branch traffic.
   Some banks have also used Mobile banking to address market segments which they have not historically been able to reach.

   Banks may expand access through use of agents to represent the bank for account opening and cash in or out services. Transactions initiated through the bank's agents are relayed back to the bank and pass over the client's account or wallet, and the bank assumes responsibility for the actions of its agents.

2. **MNO (Mobile Network Operator) Model**: A pure cell phone company (MNO) service extends the wireless network messaging functionality to provide payment services that enable customers to remit funds to each other that can be settled through the MNO's established agent network. Individual payment transactions occur entirely within the MNO and do not require the service user to have a bank account.

   The funds in transit - paid in by the remitter but not yet withdrawn by the recipient, are matched by a deposit in a segregated account with one or more banks (trust account if under common law), so are within the formal financial system.

   Since the service provider is only executing client payment instructions and is not performing the credit evaluation and risk management function of a bank, these services arguably do not constitute "banking" and do not require the level of regulatory oversight needed for deposits that are used to fund lending.

   The depository bank has no involvement in or responsibility for payments through the MNO system. Given the relatively high cost of a bank account (minimum balance, service charges, full KYC requirements, and travel time to a branch) and the easy, low

cost and increasingly universal access to cell phone services, the MNO model arguably is highly effective in brining informal cash transactions into a form of formal financial system, expanding access to financial services.

3. **Hybrid Model**: A combination of a bank, MNO or other third party that offers communications and financial transaction services that combine characteristics of both the pure bank and pure MNO models. Such combination hybrid models include but are not limited to:

    - MNO/Bank Model: Cell phone company based payment services that handle payments internally with cash in/out through the MNO's agent network, yet link to formal banking services such as savings, loans and insurance in partnership with a regulated financial institution by enabling communications with the bank and transfers between the user's cell phone payment account and accounts at the bank. Most mobile financial services are hybrid, drawing on the relative strengths of the partners involved.
    - Government Provider/Bank Model: A government sponsored interbank clearing system includes consumer access functionality, either using smart cards or smart cell phone Sims that temporarily act as a store of value and synchronize with a formal bank account. The cell phone company, if involved, provides communications services while the government operates the payment switch between banks and between accounts within banks.

## Risk Definitions

In this document, the risks discussed are only those *ADDED* by the mobile channel and associated agency banking model. These are therefore in addition to any core risks borne within a typical retail banking environment.

1. **Systemic:** A risk that could cause collapse of, or significant damage to, the financial system or a risk which results in adverse public perception, possibly leading to lack of confidence and worse case scenario, a "run" on the system and/or contagion effect
2. **Operational:** A risk which damages the ability of one of the stakeholders to effectively operate their business or a risk which results in a direct or indirect loss from failed internal processes, people, systems or external events
3. **Reputation:** A risk that damages the image of one of the stakeholders, the mobile system, the financial system, or of a specific product.
4. **Legal:** A risk which could result in unforeseeable lawsuits, judgment or contracts that could disrupt or affect MFS business practices
5. **Liquidity:** A risk that lessens the ability of a bank or MFS provider/agent to meet cash obligations upon demand

6. **Fraud:** A risk which increases the exposure of one or more stakeholders to loss of their money held within the system as a result of deliberate deception, trickery, or cheating by other stakeholders in the system.

## The Role of Mobile Network Operators and Banks

Of all the participants in Mobile Money operation, the participants with the most variable roles across differing implementations are the Mobile Network Operator (MNO) and the Banks.

The roles assumed by an MNO or bank include any or a combination of the following:

1) **Brand Provider**: This refers to the brand name carried by the Mobile Money product in the market
2) **Payment Services Provider (PSP)**: This refers to the role of managing a system which switches payment transactions on behalf of bank(s)
3) **Agent Aggregator**; this refers to the role of acquiring and managing the agency network required to perform Agency banking.
4) **Bank**: This refers to the roles of float management and transaction settlement. This role only applies to and MNO where that MNO has secured a banking license
5) **Communications bearer**: This is the role where an MNO delivers transactions to / from the Mobile Phone. For a bank to assume this role it typically needs to obtain an MNO or MVNO (Mobile Virtual Network Operator) license.

When analyzing the risk borne by an MNO or bank it is important first to analyse which of the above roles the entity is performing. In the Table below, the risks are analysed by role rather than performer of the role.

## Risk Matrix

The matrix below demonstrates the most common risks identified in actual Mobile Money and agency banking operations and maps them to the categories that may be applicable under the Basel Committee for Banking Supervision (Basel) guidelines.
The table has been limited to risks arising directly out of Mobile Money and Agency banking, and excludes those which are related to the more conventional aspects of banking, such as asset and liability management.
On account of the rapid development of the Mobile Money industry, this table is a working document which will be augmented as new risks and their mitigants are identified.

| Risk Name | Risk Description | Risk impact | Basel Risk Category | Mitigant |
|---|---|---|---|---|
| Identity theft | Sufficient elements of the customer data becomes compromised to allow another party to replicate the customer's identity in the system, thereby fraudulently using the customer's identity to conduct transactions | **Agent** – Reputational<br>**Bank** – Reputational and Fraud<br>**PSP** – Reputational<br>**Client** – fraud<br>**Brand owner** - Reputational | Operational (Level 1 category – Internal and External Fraud; Level 2 – Theft and Fraud) | Only allowing each customer to have one account in the system<br>PIN protection, and good processes for PIN resets. |
| Impersonation of provider status | An unauthorized agent acts as an authorized agent, mostly performing cash in and cash out transactions but charging fees which are not agreed to by the scheme operator, or for the purpose of confidence trickery to gain access to the customer's secret information.<br>There have also been incidents where such "agents" have defrauded the depositor and absconded with the deposited amount. | **Agent** – Reputational<br>**Bank** – Reputational and Fraud<br>**PSP** – Reputational<br>**Client** – fraud<br>**Brand owner** - Reputational | Operational (L1 – Internal and External Fraud; L2 – Theft and Fraud) | Clearly publishing the fee structure to the client, as well as consistent agent branding.<br>Agents should assist the MM provider to identify the active, but unauthorized agents in the market.<br>Clients should be educated that, unless they are notified by the Mobile Money scheme directly of any given deposit, they should not pay over their cash to the agent. |
| Inability to transact | The transactions within a mobile payments network travel through many communications systems to reach the MM backend. Any breakage in this chain can lead to an inability to transact.<br>Customer literacy levels are also a factor here. | **Agent** – Reputational<br>**Bank** – Reputational<br>**PSP** – Reputational<br>**Client** – Inconvenience<br>**Brand owner** - Reputational | Operational (L1 – Execution, Delivery and Process Management; L2 - Transaction Capture, Execution, and Maintenance) | Redundant pathways through the network need to be established as far as is possible. The MM operation should also actively test the Mobile operator's ability to deliver messages via machine generated messages on a cyclical basis.<br>Menu structures which do not change often can be used by illiterate people who learn keystroke sequences to navigate menus.<br>All transactions are to be defined with |

| | | | | |
|---|---|---|---|---|
| | | | | clear completion boundaries, thus allowing for clear rollback procedures in the event of uncertainty. |
| Transaction replay by the network | MNO's often have retry patterns to deliver an SMS to a destination. These are triggered when a send to the recipient does not generate an appropriate receipt. MM platforms which receive SMS's sometimes receive multiple copies of the same SMS bearing a transaction, which the system could interpret to be multiple instructions from the client to affect a payment. | **Agent** – Reputational<br>**Bank** – Reputational / Commercial<br>**PSP** – Reputational<br>**Client** – Loss of funds / difficulty recovering them<br>**Brand owner** – Reputational | Operational (L1 – Execution, Delivery and Process Management; L2 - Transaction Capture, Execution, and Maintenance) | Arrangements should be made with the operator to disable sms retry patterns for MM transactions. This means that a transaction will either succeed in a very short period of time or fail, leaving the customer in a more sure position after transaction submission.<br>Transaction requests should also be numbered at source by the MM menu on the phone, and the back end system should only post a given transaction request once. |
| Relationship difficulties between the owners of the service – leading to service outage | MM products are often delivered by consortia of mobile operator(s), bank(s) agent network manager(s) and agents. These consortia are often serviced by third party software vendors whose support is critical for systems changes. Any significant relationship difficulty within this consortium could result in service unavailability to a client or to all clients. | **Agent** – Reputational and commercial<br>**Bank** – Commercial<br>**PSP** – Reputational and commercial<br>**Client** – Inconvenience through loss of service<br>**Brand owner** – Reputational | Operational (L1 – Execution, Delivery and Process Management; L2 – Vendors and Suppliers) | The relationships need to be carefully planned at service inception to ensure that all parties are adequately reimbursed for their participation in the process. The MM provider needs to retain a position of consortium leadership to ensure that all parties remain committed to the product. |
| Transaction delayed by network | Message delivery through a mobile network takes place via multiple interconnected systems. At each point in the chain delays are possible. Any delay in transmission leaves the customer and agent in a difficult | **Agent** – Reputational<br>**Bank** – Reputational<br>**PSP** – Reputational<br>**Client** – Inconvenience and | Operational (L1 – Execution, Delivery and Process Management; L2 - Transaction | Arrangements should be made with the operator to disable sms retry patterns for MM transactions. This means that a transaction will either succeed in a very short period of time or fail, leaving the customer in a more |

| | | | | |
|---|---|---|---|---|
| | position of not knowing whether or not the transaction has been delivered, and therefore whether or not to re-submit the transaction. | the risk of incorrectly making the same payment more than once<br>**Brand owner** – Reputational | Capture, Execution, and Maintenance) | sure position after transaction submission.<br>Agent and customers should also be educated to confirm balances where there is uncertainty regarding completions of a given transaction. |
| Insufficient points at which to use Mobile Money leading to customers withdrawing from the service | A pure mobile money offering seldom has access to any parts of the existing payments system, which means that many of these payment destinations need to be re-created for the mobile money operation. Any client who takes up the product before a significant number of these points has been activated will find little use for the product | **Agent** – Reputational, insufficient business volume<br>**Bank** – Commercial<br>**PSP** – Reputational, insufficient business volume<br>**Client** – Inconvenience<br>**Brand owner** – Reputational | Strategic Operational (L1 – Execution, Delivery and Process Management; L2 – Vendors and Suppliers) | The product rollout needs to be managed as a network product, ie agents, bill pay recipients, merchant payment locations etc need to be rolled out in a geographically harmonized manner.<br>Rolling out a card in conjunction with the mobile money product may also enable access to existing payment system resources. |
| Lack of cash or electronic float at agent outlet | A client wishing to deposit or withdraw money to the system may be temporarily or permanently unable to do so on account of the agent not having sufficient cash or electronic float to perform a transaction. | **Agent** – Reputational, insufficient business volume<br>**Bank** – Commercial<br>**PSP** – Reputational, insufficient business volume<br>**Client** – Inconvenience<br>**Brand owner** – Reputational | Liquidity | Agents need to be rolled out in conjunction with consumers, and need ongoing management to ensure that there are no e money shortfalls at the agent locations.<br>Agents need to adequately fund this line of business in terms of cash and electronic float.<br>Ongoing systems monitoring is also crucial to prevent systems outages from preventing access to the agent's electronic balances. |
| Abuse of customer details by any member of the supply chain | MM operations often rely on networks of agents, managed by agent network managers to gather customer details for KYC. Any | **Agent** – Reputational<br>**Bank** – Reputational<br>**PSP** – Reputational | Operational (L1 – Execution, Delivery and Process | Rapid collection of original documentation from the network may reduce the incidence of this type of fraud. |

| | | | | |
|---|---|---|---|---|
| | member of this chain with access to the customer registration details could use these details for other fraudulent purposes. | **Client** – Fraud<br>**Brand owner** - Reputational | Management; L2 - Transaction Capture, Execution, and Maintenance) (L1 – Clients Products and Business Practices; L2 – Selection, Sponsorship and Exposure) (L1 – Internal and External Fraud; L2 – Theft and Fraud) | Agents need to be vetted for character during their appointment process. Clear and direct action in the event of occurrence will also mitigate against recurrence. The agent needs to implement stringent customer detail management processes in its outlets. |
| Delays in balance updates by the service | Given the length of the chains of message handling within Mobile Money operations, balance updates may be delayed for any given transaction. This exposes the customer to future transactions possibly being incorrectly declined due to "insufficient funds" or to unexpected overdrafts if a withdrawal transaction is delayed. | **Agent** – Reputational<br>**Bank** – Reputational<br>**PSP** – Reputational<br>**Client** – Inconvenience<br>**Brand owner** - Reputational | Operational (L1 – Execution, Delivery and Process Management; L2 - Transaction Capture, Execution, and Maintenance) | All efforts must be made to shorten the message delivery paths through the network, and to give the priority over network components. MM platforms must be adequately scaled to support the customer numbers enrolled. The systems need to be designed with clear transaction commitment points which lead to balance updates. These should also support clear confirmation, failure and roll-back mechanisms. |
| Receipt of counterfeit notes from customers | In most Mobile Money implementations, the agent cash in transaction takes the form of an exchange of cash for electronic float at the point of sale. If the client | **Agent** – Commercial<br>**Bank** – Commercial<br>**PSP** – None<br>**Client** – Inconvenience | Operational (L1 – Internal and External Fraud; L2 – Theft and Fraud) | Training in the detection of counterfeit money linked to processes which ensure its application in transactions. |

| | | | | |
|---|---|---|---|---|
| | should successfully tender counterfeit funds in exchange for electronic float, the overall integrity of the system will not be compromised, but the agent will lose the corresponding amount of electronic float.<br>This may result in the agents, their agent managers and any banks which supply cash management services to the Mobile Money operation, withdrawing their support for the Mobile Money operator. | **Brand owner** – Reputational | | |
| Burglary of cash float | Accepting cash in transactions at point of sale may increase the float size within a given retail outlet. This additional cash may increase the likelihood of burglary attempts at the point of sale.<br>This may result in the agents withdrawing their support for the Mobile Money operator. | **Agent** – Commercial<br>**Bank** – Commercial<br>**PSP** – None<br>**Client** – Inconvenience<br>**Brand owner** – Reputational | Operational (L1 – Internal and External Fraud; L2 – Theft and Fraud) | Stocks of cash need to be kept small enough to remain uninteresting to criminal gangs, while simultaneously maintaining enough cash stock to cover the activity level in the agent. |
| Split transactions | In many Mobile Money implementations, proportionally risk adjusted AML procedures have been applied to extend the service to the un / under banked. These adjusted AML requirements are normally counterbalanced by transaction volume and value restrictions placed on the account.<br>To circumvent these controls, the client may be tempted to split large transactions into several smaller ones | **Agent** – None<br>**Bank** – Fraud<br>**PSP** – None<br>**Client** – Fraud<br>**Brand owner** - Reputational | Operational (L1 – Internal and External Fraud; L2 – Theft and Fraud) | AML software should be deployed to check for clusters of transactions and to flag these up to the risk departments of the bank or MMO as suspicious.<br>These are then managed by the risk department on an exception basis. |

| | | | | |
|---|---|---|---|---|
| | which fit within the definition of the restrictions applied. | | | |
| Spoofed transactions being used to make cash withdrawals | Depending upon the security level of the underlying system, it may be possible for people posing as clients of the MM solution to inject notifications to the merchant which appear to be cash withdrawal approvals. If these are acted upon the resultant cash paid out will be lost by the agent<br>This may result in the agents withdrawing their support for the Mobile Money operator. | **Agent** – Fraud<br>**Bank** – Commercial / fraud<br>**PSP** – Reputational<br>**Client** – Fraud<br>**Brand owner** – Reputational | Operational (L1 – Internal and External Fraud; L2 – Theft and Fraud) | The Mobile Money system needs to have sufficient inherent system security features to minimize these types of technical attacks.<br>Examples of this include anything from end to end transaction encryption and mac'ing to keeping the agent's mobile number secret and requesting that the MNO block SMS header spoofing.<br>The agent also needs to train its staff to focus on the transactions to ensure that they are valid. |
| Teller counting errors during cash in and cash out operations | If the teller miscounts the amount of cash deposited or withdrawn, the resultant shortfall / surplus will accrue to the agent<br>This may result in the agents withdrawing their support for the Mobile Money operator. | **Agent** – Commercial<br>**Bank** – Commercial<br>**PSP** – none<br>**Client** – Commercial<br>**Brand owner** – Reputational | Operational (L1 – Execution, Delivery and Process Management; L2 - Transaction Capture, Execution, and Maintenance) | The tellers need to maintain vigilance. |
| Mobile money program fails to reach sustainability | If the Mobile Money program as a whole fails to reach the point of commercial sustainability, the sponsors may withdraw. | **Agent** – Reputational and commercial<br>**Bank** – Reputational and Commercial<br>**PSP** – Reputational<br>**Client** – Inconvenience<br>**Brand owner** - Reputational | Strategic Operational (L1 – Execution, Delivery and Process Management; L2 – Vendors and Suppliers) | The MM operator needs to ensure that the system overall grows at a suitable pace. |
| Too many short term | Mobile Money operations can grow | **Agent** – none | Liquidity | Diversify the product, to add savings |

| | | | | |
|---|---|---|---|---|
| deposits | very quickly, attracting substantial, but short term deposits. | **Bank** – Liquidity<br>**PSP** – none<br>**Client** – none<br>**Brand owner** – none | | capabilities, as well as short tem lending. |
| Insolvency of the underlying float provider | A typical MM product is a "deposit and pay" service, meaning that the customer has deposited funds into the system. These funds are typically held by a licensed bank. It is possible that the underlying bank could face financial difficulties, placing the customer deposit at risk. | **Agent** – Commercial<br>**Bank** – Commercial<br>**PSP** – Reputational<br>**Client** – Loss of funds<br>**Brand owner** – Reputational | Credit | Regulators need to watch the capital adequacy of the float holders carefully as mobile money has the potential to create concentration risks within the economy.<br>Diversification of deposits into multiple banks is an effective mitigant.<br>Mobile Money operators need to partner with responsible banks to ensure that the float will be managed appropriately. |
| Relationship difficulties between the owners of the service – leading to service outage | MM products are often delivered by consortia of mobile operator(s), bank(s) agent network manager(s) and agents. Any significant relationship difficulty within this consortium could result in service unavailability to a client or to all clients. | **Agent** – Commercial<br>**Bank** – Commercial<br>**PSP** – Reputational<br>**Client** – inconvenience / Loss of funds<br>**Brand owner** – Reputational | Operational (L1 – Execution, Delivery and Process Management; L2 – Vendors and Suppliers) | The relationships need to be carefully planned at service inception to ensure that all parties are adequately reimbursed for their participation in the process. The MM provider needs to retain a position of consortium leadership to ensure that all parties remain committed to the product. |
| Lack of clarity as to who holds customer money | Mobile Money products are often offered under another brand (such as that of an MNO) and the client may not be aware of the licensed financial entity which actually holds his / her funds. This could make enforcing rights more complicated for the client. | **Agent** – Reputational<br>**Bank** – Reputational<br>**PSP** – Reputational<br>**Client** – inconvenience / Loss of funds<br>**Brand owner** – | Credit | All marketing communications with the client should clearly explain to them who the bank of last resort in the system really is. This enables the customer to access consumer protection capabilities within the country. |

| | | | | |
|---|---|---|---|---|
| | | Reputational | | |
| Keystroke errors | Keystroke errors could result in the client paying incorrect beneficiaries or paying an incorrect amount, or both. | **Agent** – None<br>**Bank** – Re-work<br>**PSP** – None<br>**Client** – inconvenience / Loss of funds<br>**Brand owner** – Reputational | Operational (L1 – Execution, Delivery and Process Management; L2 - Transaction Capture, Execution, and Maintenance) | In many Mobile Money applications, the customer telephone number is used as the primary identifier of the customer. Adding and processing a check digit into the customer mobile number to make the account number decreases the likelihood of an incorrectly captured number being accepted as a beneficiary number.<br>The Mobile Money operation needs to provide customer with a redress process in the event of incorrect beneficiary data capture. |
| Fraudulent use of mobile number | Mobile numbers are aliases for the customer IMSEI within the GSM networks. These can therefore be re-appropriated within the network, or the number can be appropriated in the street via handset or sim card theft. | **Agent** – None<br>**Bank** – Fraud<br>**PSP** – None<br>**Client** – Fraud<br>**Brand owner** – Reputational | Operational (L1 – Internal and External Fraud; L2 – Theft and Fraud) | Pin security is key for managing this risk. To prevent network centered replay, encryption of the pin, to a higher standard than the GSM native encryption, within any SMS messages is also recommended. |
| Fraudulent use of customer details to establish a loan | Agents acting alone or in collaboration with external entities may use fraudulent customer details to secure a loan | **Agent** – Fraud<br>**Bank** – Fraud<br>**PSP** – None<br>**Client** – Fraud<br>**Brand owner** – Reputational | Operational (L1 – Internal and External Fraud; L2 – Theft and Fraud) | The bank should only lend to customers with a stable transaction history with the Mobile Money operation<br>The bank should validate the data provided by the agents via credit scoring agencies and by direct contact with the customer |
| Reduction in level of relationship between the bank and the customer | On account of the complex branding and distribution structure, the client may have no relationship with the lender, and may therefore feel a diminished obligation to repay loans | **Agent** – None<br>**Bank** – Loss of funds loaned<br>**PSP** – None<br>**Client** – relationship | Credit Risk | The lender needs to closely monitor repayment patterns and respond quickly to unexpected behavior by the client. |

| | | | | |
|---|---|---|---|---|
| | granted to him / her | **Brand owner** - None | | |
| Improper verification of KYC information during account registration | Agents are typically reimbursed for their activities via commissions paid for new accounts opened. This may make them less diligent in checking the customer's KYC information while registering a new customer account | **Agent** – Reputational / relationship<br>**Bank** – Reputational / commercial<br>**PSP** – None<br>**Client** – Inconvenience / loss of funds<br>**Brand owner** - Reputational | Operational (L1 – Execution, Delivery and Process Management; L2 – Monitoring and Reporting) | Depending on the regulation customer accounts can be opened with limited services until KYC identification can be confirmed. The operator can leverage databases to confirm ID matches and official black list reports to reduce the risk of fraudulent and criminal accounts. Education of agents is critical to quality, as is delayed commission payments, agent irregularity reporting and commission claw back rules that reduce this risk<br>In the case of remittance transactions, The value of remittance transactions originated via OTC channels should be kept low enough to prevent systemic and money laundering damage.<br>The Bank under whose auspices the transactions are conducted should conduct spot checks on the transactions submitted as well as tracking behavior of the agents.<br>Ongoing agent training is essential |
| Improper data capture by agents during OTC remittance transactions | Data capture errors made by the agent may result in misdirected remittance transactions | **Agent** – Reputational / relationship<br>**Bank** – Reputational / commercial<br>**PSP** – None<br>**Client** – Inconvenience / loss of funds<br>**Brand owner** - | Operational (L1 – Execution, Delivery and Process Management; L2 - Transaction Capture, Execution, and Maintenance) | Customers remitting to the same recipients multiple times should be encouraged to pre-register their beneficiaries<br>Remitting banks should validate the remittance fields (such as account number and name)<br>Full details of recipients should be obtained from the remitter and should be validated by the pay out station |

| | | | | |
|---|---|---|---|---|
| | | Reputational | | prior to cash out |
| System and Bank Pool Account Variances | The funds under management in a mobile money system are reflected in a corresponding 'pool' bank account. The mobile money system mainly comprises of payments within the 'closed loop' of the system. These intra-system value transfers do not impact total value within the system. However external payments into the system (e.g. payroll & G2P) & out of the systems (3rd party bank ATM withdrawals, & bill-payment), require 'system-value' adjustments. The adjustments need to be reflected in corresponding bank pool account. The risk is that there is a variance between the two values | **Agent** – None<br>**Bank** – Liquidity<br>**PSP** – None<br>**Client** – Inconvenience / loss of funds<br>**Brand owner** - Reputational | Operational (L1 – Execution, Delivery and Process Management; L2 - Transaction Capture, Execution, and Maintenance) | Mobile money system integration into bank pool account so all changes to main bank account is reflected. End of day variance reports to managed and signed off by appropriate business management.<br><br>If manual system value changes are required. Robust system authority approver & checker function is required by operator & bank personel |

## Acknowledgements

The author would like to thank the following people for their assistance and guidance in the definition and editing of this paper:

1. Cameron Evans, Principal Financial Officer, International Finance Corporation
2. Paul Reynolds, Consultant, International Finance Corporation
3. Michael Joyce, Mobile Money Policy Advisor, National Team for the Acceleration of Poverty Reduction in Indonesia

# Appendix A - Emerging market level fraud attacks on Mobile Money operations - An excerpt from the Observer (Kampala, Uganda)

Downloaded from http://allafrica.com/stories/201309110140.html?viewall=1

## Uganda: How Billions Are Lost in Mobile Money Fraud

By Zurah Nakabugo & Shifa Mwesigye, 10 September 2013

MTN Mobile Money, Orange Money, WaridPesa, Airtel Money and M-Sente are some of the mobile money services affected. A source in the police public relations office admitted that they are struggling to catch up with the criminals behind the scam.

"Because of so many unregistered Sim cards, it's very hard to track suspects and arrest them. Other conmen use fake details to register Sim cards used in mobile money fraud," the source said.

**Fraud at work:**

Timothy Arinanye, 32, a mobile money agent lost Shs 3.5m to a conman last Wednesday. He says that a client with telephone number 0783860927 wanted to deposit Shs 356,600 onto his account.

"When my employer gave this conman the phone to put the pin number, he transacted Shs 3,566,000 and sent it to his phone. We realised it in the evening when balancing the sales," he said.

Arinanye adds that when he called the number, the owner denied receiving it and switched off his phone. The case is registered at police under case Ref.SD 17/05/09/2013.

"When I contacted MTN to block the money which was deposited on that account, they told me they can't do it unless I get a court order since the suspect is also their client. By the time I got the court order, the money had been withdrawn and the phone switched off. It will never be recovered," says Arinanye.

With a bank loan to clear and no more start-up capital, Arinanye's business collapsed.

**Pin code:**

In another trick, conmen master the agent's pin code by giving him an invalid number which he repeatedly dials while entering his code. When he gives the fraudster the phone to type in the correct number, he sends all the agent's money to himself and disappears. The agent realises later that he was robbed.

Another victim, Cissy Namayanja, says she received a call from 0704300989 and a man claimed he had credited her account by mistake.

"I checked my account and there was no credit. After like two minutes, the person called again inquiring whether I had received a message. I realised the message had just come in saying, 'You have received 850,000'.

He said that he was an agent who was sending money to a client and that I should reverse the transaction from my side. He asked whether I had any money on my account to which I said yes. He proceeded to give me a code and finally told me the transaction was hanging since I needed more money on my account as transfer charges.

The message I got on the screen meant nothing and this guy never credited my account in error but wanted to access what I had using the code he provided. I don't know how those messages work but I didn't even think of checking my account balance first. I think the screen message I read facilitated him to withdraw the money," Namayanja says.

Other fraudsters go to mobile money agents while driving expensive vehicles and pretend to be rushing. They ask for a deposit of huge amounts, say Shs 3m. After sending, they give the agent fake currency and distract him so that he doesn't realise the fake money. By the time you realise it is fake, the fraudster has vanished.

**Network busy:**

The thugs also take advantage of network problems in an area to deposit money on their phones. When the agent gives them his phone to enter the mobile money pin code, they send the money quickly but delete the sent message and tell the agent that indeed the network is off and disappear without paying.

Armed with a fake message that shows funds on the phone, a fraudster can pretend to be in a rush and ask the agent to give him cash but retain the phone to withdraw the money he has taken when the network resumes.

Conmen also use the MTN back-up customer service for contacts or Sim card registration by pretending to be employees backing up or registering Sim cards. After swapping your card with another, they use it to commit crimes. When police tracks the line, an unsuspecting victim is arrested.

Fraudsters are also targeting money transfer agents such as Western Money Union and Money Gram.They hack emails and get all the details of the sender and receiver. They forge the identification of the receiver and then withdraw the money. By the time the rightful owner goes to claim the money, the fraudster is targeting his next victim.

**Telecoms employees:**

Many mobile money users don't know how to check the balance on their phones and think receiving a message is actual money sent to them. Some thieves are now claiming to be priests or pastors who erroneously sent money meant for orphans.

Many people do not know how to send back money from their phones to another person. Some rely on agents to help them send money and even disclose their passwords to agents. They then realise later that no money has been sent to you and yet you have already sent them your own money.

According to police, some of the fraudsters are former employees of telecom companies, who connive with current employees to withdraw money from accounts with huge sums.

"We are investigating a case where a woman left Shs 100m on her mobile account at night. By morning, the money was deposited on a different mobile account and withdrawn," our police source told us.

**Mobile money agents are the biggest target of fraudsters posing as customers.**

"We get so many cases of such victims everyday but the mobile telecom companies have failed to cooperate with police and give us particulars of the suspect immediately to act fast and arrest him. Getting a court order to block the phone takes two to three days and by this time the money has already been withdrawn," the source explains.

"The telecom companies can't give police the particulars of the suspect unless they apply for a mobile money printout statement which takes between five days to two weeks to get. It costs Shs 30,000 at MTN and Shs 20,000 in other telecom companies. It takes long to get the printout because most of the times the network is off and there are long queues," the source adds.

Even with a printout, telecom companies give only the telephone number of the suspect, withholding details such as name and photograph. This makes it difficult for police to track the suspect. He says numbers are registered in abbreviations like WMJG JSM or Tpg TSM. One could be registered as Rose Nabitalo yet the actual owner of the phone is Uthuman Kimalo.

"I don't see any impact of telecom companies in registering Sim cards if they can't reveal all the particulars of suspects to police to arrest criminals," the source adds.

Kampala Metropolitan Police Spokesperson Ibn Ssenkumbi said they want telecom companies and Uganda Communications Commission to freeze the accounts that receive the stolen money until investigations are completed.

UCC communications manager Fred Otunnu says mobile money will be streamlined with Bank of Uganda under the Financial Institutions Act.

"We shall highlight all the issues affecting the mobile money business to improve services," he said.

Ronald Lwasa Mpijja, the investigating officer of Mobile Money fraud at Kampala Central Police Station, says their main suspect is one Kenneth Olinawe with telephone number 0777556820.

He said according to their investigations, some fraudsters are in a racket using one phone with different Sim cards to con mobile money agents.

"It has been proven by the mobile money printout which indicates the same serial telephone number used by different Sim-cards in stealing the money. They use one phone to commit several crimes," Lwasa said.

He added that police are hunting down the owners of telephone numbers used in mobile money fraud.

## Appendix B – Employee fraud attacks on Mobile Money operations - An excerpt from the Observer (Kampala, Uganda)

Downloaded from: http://www.finextra.com/news/fullstory.aspx?newsitemid=23759

# Ugandan telco says employees stole $3.5m in mobile money fraud

28 May 2012 | 7502 views | 4

Telco MTN Uganda has confirmed that employees have stolen around US$3.5 million from an account used to store cash incorrectly sent through its mobile money transfer service.

Responding to local press reports, the company has confirmed that members of staff "took advantage of gaps" that emerged during a systems upgrade to pilfer USh9 billion.

The money was taken from a "suspense account" used to store cash from incorrect transactions - where customers have entered the wrong details.

In a statement given to local news outlet The Observer, MTN says that customer money is not affected and that following an internal investigation it has "instituted disciplinary and criminal proceedings against a number of its employees".

According to The Observer, MTN has already fired Richard Mwami, head of public access and mobile money who has protested his innocence and sued the company for wrongful dismissal.

"With further upgrades and modifications undertaken to increase its robustness, MTN is confident that it has brought the Mobile Money system to high levels of stability and security," says the statement.

Uganda: How MTN Lost Mobile Billions - The Observer