GSMA Mobile Money for the Unbanked

Managing the Risk of Fraud in Mobile Money

Authors: Lara Gilman and Michael Joyce

Executive summary

Risk management is a key component to the commercial success of any business. Effective risk management underlies sustainable commercial growth because it protects two key commercial assets: reputation and revenue.

Mobile operators are familiar with managing risks on the GSM side of the business and those that have launched mobile money are aware that mobile money carries different kinds of risk – particularly the risk of fraud. This paper outlines a framework to managing fraud and risk. The four key elements of that framework are: (i) determine risk appetite; (ii) identify and assess risks; (iii) establish effective controls; and (iv) monitor and review the risk management strategy.

In our research, MMU found that operators are aware of the need to develop a robust risk management strategy for mobile money. This paper will highlight some effective practices that operators use to manage the risk of fraud in order to assist mobile money providers as they continue to review and enhance their risk management strategies.

Introduction

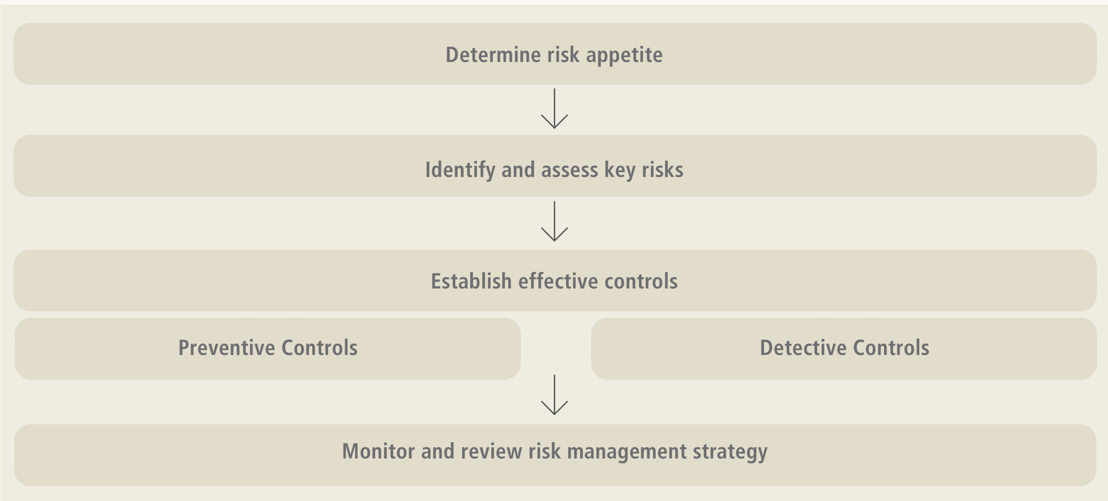
Managing risk in mobile money is a challenging task, especially when it comes to the risk of fraud. Fraud not only results in financial loss to customers or a mobile money provider, but it also damages the reputation of the service to the customer and risks the reputation of the industry as a whole. As such, mitigating the risk of fraud is a primary objective in a robust risk management strategy.

In practice, MNOs, banks and third parties recognize that risk management is an essential pillar to the sustainable commercial success of a mobile money deployment. As MMU has addressed in other publications, mobile money is anything but a quick and easy value-added service (VAS). Operators with effective risk management strategies are aware of the complicated nature of mobile money and have invested dedicated resources to manage the fraud and revenue assurance activities.

However, specific risk management strategies vary from operator to operator. Strategies are affected by numerous factors including stage of development, organisational structure, number of product offerings, regulatory environment and local market context.

While the structure of managing fraud may differ, there is a common framework that is widely agreed to be the foundation to any risk management strategy in mobile money. The framework is composed of four elements that mobile money deployments use to manage risk: determine risk appetite, identify risks, establish controls and monitor effectiveness. The diagram below is a visual representation of the framework and is a guide for topics covered in this paper.

This risk management framework is not far from ISO 31000:2009[1] or SOX[2] standards which are global guidelines on risk management. As such, it could apply to many industries but our focus is how it is used in the mobile money context in order to highlight how operators mitigate the risk of fraud in mobile money. Other risks including compliance, business continuity, health and safety, and physical theft are beyond the scope of this paper and will not be specifically addressed.



1 ISO Standard 31000:2009 (Risk Management – principles and guidelines) was consulted in the preparation of this paper, but the framework presented here differs in several aspects. Risk managers developing risk documentation and frameworks for their organisations should consider any local regulatory requirements as well as international standards such as ISO 31000.
2 US Sarbanes-Oxley Act 2002, a US law on financial responsibility.

Determine risk appetite: the foundation of risk management

To successfully prioritise and control the risk of fraud, mobile money operators need to understand their risk appetite, which is a way of expressing what costs they would be comfortable to carry. Every risk will have a cost, as will any control. A mobile money deployment that is more conservative may be inclined to avoid risk and be more willing to accept slower growth or higher operational costs. Alternatively, a deployment that is more focused on rapid expansion and innovation will be more open to accepting a greater risk exposure. What is important is that mobile money managers and those responsible for commercial growth have guidance on appropriate levels of risk when developing commercial strategies or exploring new service offerings.

In the same way that the risk appetite of mobile money deployments may vary, so too do the methodologies used in determining risk appetite. Some operators may attempt to define a quantitative risk appetite (for example, for less than a certain percentage of transactions to be subject to frauds or complaints). Others may use a qualitative scale, such as defining risk appetite levels as averse, minimalist, cautious, open, or hungry.[3]

Support for developing risk appetite could originate from a number of players. We have seen some deployments that rely on their bank partner for guidance on an appropriate risk appetite level. Other deployments use more group level support while some deployments develop their risk appetite through the fraud and revenue assurance team that manage the GSM side of the business. While this step in the process may be somewhat conceptual, it is an important one in order to be in a position to create effective and relevant controls.

Identify and assess key risks: understanding the potential of fraud

Orange Group: The first steps to managing risk in mobile money

Prior to the launch of Orange Money, Orange Group knew that they had to look at this new service with a fresh eye. While the commercial and marketing teams evaluated the direct and indirect potential benefit of launching mobile money, the corporate fraud and revenue assurance team needed to identify and assess the risks of a complicated new service. For Orange, the most important objective was to protect the interests of Orange Money customers from fraud, while also ensuring the service remained accessible and easy to use. Orange recognised that a robust risk management strategy would be foundational to building trust with customers.

The team's first step in understanding how to manage risks in mobile money was to analyse the vulnerabilities of the service. In addition to relying on the wealth of their own experience from the GSM business, the fraud team sought support from outside experts and proxy industries, such as other financial and payment services. Building up a portfolio of potential frauds, Orange was better equipped to develop processes and thresholds to mitigate the risks of mobile money.

The benefit of creating a strategy from scratch is that it allows the operator to tailor the strategy to the requirements of the service. Mobile money is inherently complicated requiring controls and processes beyond the GSM business. For any new deployment, the prospect of building a strategy from scratch may seem slow but it is necessary. The first step to building that strategy is to identify and understand the vulnerabilities in the mobile money service.

In order to build an effective risk management strategy, operators need to identify the vulnerabilities in the operations of its deployment. The risk identification process is often conducted by those responsible for the risk management of the business as a whole, such as a revenue assurance team. For example, we have seen at least a couple of MNOs who have created a review process for any new product for their mobile money service. As part of the review, any new product or pricing must be reviewed by all stakeholders in the business including sales, marketing, distribution, finance and security and revenue assurance. The security and revenue assurance team identify and evaluate the probability of risk and estimate the impact. While this is not the only model in the industry, it is important to note that the responsibility for identifying risks has been clearly designated to a specific team.

So, where are some of the key risks of fraud in mobile money?

There are risks that exist in every mobile money service around the world, such as the potential theft of customer information or manipulation in e-money reconciliation. However, as fraudulent activity varies from deployment to deployment, it is more relevant to look at risk identification from a payment ecosystem perspective. In other words, where in the mobile money process might actors or participants be at risk or capable of committing fraud? The key players who need to be considered are the customer (transactional risk), the agent (channel risk) and the employee (internal risk).

3 "Thinking about risk: managing your risk appetite: a practitioner's guide." HM Treasury, November 2006.

Potential frauds in mobile money

Transactional	Channel	Internal
■ **Vishing/Smishing**: Use of phone calls or SMS to gather personal details such as account numbers, PINs or personal identification details. ■ **Advance Fee scams**: Customers duped to send funds under fake circumstances or promises. ■ **Payroll fraud**: Non-existent or "ghost" employees receiving funds. ■ **Reversal Requests**: Customer requests to reverse transactions that were in fact successful. ■ **False transactions**: Sending fake SMS to make customers believe a transaction was successful. Often accompanied by a reversal request.	■ **Split transactions:** Agents split cash-in transactions in order to earn multiple commissions (only applies to tiered commission structure). ■ **False transactions:** Agents transferring customer funds to personal account. ■ **Registration Fraud:** Creation of accounts for false, invalid or duplicated customers for the purpose of obtaining extra registration commissions.	■ **Internal fraud:** Employees colluding for unfair personal financial gain. ■ **Identity theft:** Employees accessing and exploiting customer information without authorisation.

By looking at each player, operators can identify and assess the vulnerabilities in the system. For example, customers are often the victim of fraud because they have not adequately protected their PIN. Within the channel, agents could exploit the system by splitting transactions for unfair gain. While this may not be characterised as fraud in a legal sense, operators often treat it as fraud since it has the same effect for the revenue line of the business. Internal risk, or the risk of an employee defrauding the company, is critical to understand because the financial and reputational exposure can be huge even if the likelihood may be low. Mobile money deployments with effective risk management strategies have been meticulous in reviewing any of the vulnerabilities, especially the e-money reconciliation process, which could enable employees to defraud the company. Identifying the risk of fraud from the perspective of all the stakeholders involved provides the mobile money operator an end-to-end understanding of the risks that need to be managed.

Once the risks have been identified, they should be compared to the established risk appetite. Any risks which fall outside the risk appetite of the company will need further investigation and controls will need to be put in place to manage or reduce these risks until they are acceptable to the business.

Questions to consider when identifying and assessing operational risks in mobile money

- What are the most complex parts of the process?
- Are there any large value, high-risk transactions that happen regularly?
- Are there any authentication mechanisms that are easily faked?
- How could someone abuse the system?
- How could someone disrupt operations?
- What frauds are prevalent in the country apart from mobile money? How common are they?
- What is the general level of criminal activity and the strength of law enforcement in the country?
- What is the likelihood of the risk?
- What is the potential impact on the business (financial and reputational)?

Establish effective controls: mitigating the risk of fraud

With the key risks identified, the next step for a mobile money operator is to establish effective controls, which is a cost-effective action or policy to manage specific risks. A successful control will underpin, but not block, sustainable commercial growth.

Using controls to mitigate risk in mobile money

Controls in mobile money are either preventive which reduce the likelihood of fraudulent activity or are detective which monitor and report trends or activities that have already happened. In Table 1, we have outlined the key controls as they affect most mobile money deployments.

While this is not a comprehensive list, each of these controls addresses at least one specific risk associated with mobile money. For example, controlling access rights helps to reduce the risk of theft of customer information, while monitoring and analysing suspicious transactions increases the visibility of fraudulent activity.

Table 1: Examples of controls in mobile money

Preventive Controls	Detective Controls
■ Control access rights to protect customer information ■ Segregation of duties to reduce error or fraud on high risk procedures (e.g: e-money reconciliation) ■ Threshold limits to reduce risk associated with AML/CFT ■ Customer awareness campaigns to increase customer education and protection ■ Agent training on acceptable practices and terms and conditions ■ Employee training on roles and responsibilities	■ Monitor and analyse suspicious activity ■ Monitor activity on system access ■ Create robust customer recourse and escalation procedures ■ Monitor agent transaction activity ■ SMS alerts to customers ■ Management review of high-value transactions

Preventive controls are generally held to be stronger than detective controls, especially if these controls can be implemented as technical features of the mobile money system. If controls such as segregation of duties, access rights or network hardening are deployed, it is important for these controls to be implemented robustly, with proper documentation, review and testing. If the controls are in place but are easily circumvented (for example, if segregation of duties is in place but users commonly share passwords to get around it), risks of fraud still remain.

The size of the deployment and availability of resources can have an impact on whether a deployment relies more on preventive or detective controls. For example, in smaller deployments where resources may be more limited, there may be more emphasis on monitoring activity especially considering that the volume of activity tends to be lower. Larger deployments, such as Telenor Pakistan's Easypaisa, with higher transaction volume and multiple product offerings, have developed a more balanced approach and rely heavily on both preventive and detective controls. All mobile money deployments should continue to review the effectiveness and relevance of controls, particularly as the deployment grows both in customer base and volume of transactions. Controls that are suitable for a smaller and younger deployment will need to be reviewed as the deployment grows commercially.

Telenor Pakistan Easypaisa: Using controls to manage agent arbitrage

Tiered commission models allow agents to derive greater benefit out of low value transactions, which is critical in mobile money deployments where low value transactions drive the business. Easypaisa decided to pursue a tiered pricing model to take advantage of these commercial benefits. However, tiered commission models are inherently riskier than percentage-based models with more opportunities for agents to "game" the system through splitting transactions to earn multiple commissions.

Rather than abandon the benefits of the tiered commission model, Easypaisa implemented a preventive and a detective control to mitigate the risk. Both controls required Easypaisa to conduct analysis on customer activity. They discovered two helpful facts to create controls suited to the specific requirements of their service. Firstly, normal customer behaviour was to deposit at least 50 Rupees into their Easypaisa account at any one time. Secondly, the team determined that over a 15 day period, any account making more than 45 cash deposits (average of three deposits per day) was abnormal and often linked to suspicious activity.

Identifying "normal" vs. "abnormal" behaviour meant that the Easypaisa team was able to create controls that could be effective but not excessive. Knowing that customers deposit at least 50 Rupees meant that Easypaisa could create a minimum deposit that would not detract from the customer experience but would make it more difficult for agents to split transactions. Equally, by understanding the patterns of "abnormal" behaviour, Easypaisa could develop a detective control where they created reports to highlight any accounts performing more than 45 cash deposits at the same agent point in a 15 day period. By creating these controls, Easypaisa was able to take advantage of the commercial benefits of tiered commissions while managing their level of risk exposure.

Tools to ensure successful controls: data, communication and clearly defined internal procedures

There are three tools that mobile money deployments use in order to effectively implement controls:

1) Reliable and relevant data and dashboards.
2) Clear reporting and communication channels between stakeholders, including customers.
3) Internal procedures that define how to escalate awareness and action upon detection of suspicious activity.

Data is an important asset when it comes to managing and monitoring fraud in mobile money. Monitoring transactional activity is a key benchmark in an effective strategy, but there is no one single dashboard that will be able to be adopted by all mobile money deployments. Reliable data comes from working with back office teams and/or platform providers. Looking again how Easypaisa manages agent arbitrage, they needed to uncover locally relevant facts that they could use to determine normal and abnormal behaviour.

Safaricom M-PESA: Communication as a preventive control – a look at customer awareness

One of the top priorities for Safaricom's M-PESA is mitigating the risk of scams against customers. Rather than attempt to only use detective controls, Safaricom relies heavily on a preventive control to reduce risks of scams against customers. Safaricom has found the most effective preventive control is raising customer awareness through clear communication. To reach M-PESA customers, Safaricom uses a multi-pronged approach. SMS blasts, radio announcements in local dialects, local skits and newspaper ads are all part of their customer awareness campaigns. Increasing customer awareness through clear communication has been vital to Safaricom's success in managing fraud against M-PESA customers.

Communication, internal and external, is the second tool that mobile money deployments need to use to enforce effective controls. Depending on the number and complexity of controls that have been established, there might be numerous stakeholders in the process. Internally, mobile money managers, back office support, customer service, and finance and revenue assurance teams are some of the common stakeholders that need to be aware and encouraged to communicate any anomalies or suspicious activity to relevant internal parties.

External communication to agents and customers is equally important for an effective preventive control. Creating awareness among customers about how to avoid the risk of fraud is a critical preventive control to reduce prevalence of customer scams, as we see in the case of M-PESA.

Finally, when a fraud or suspicious activity is detected, **internal procedures need to be in place in order to ensure suspicious activities are escalated appropriately**. Internal procedures need be comprehensive so that information is shared and appropriate action follows. When a customer calls to complain that funds in their account have disappeared, the customer service centre needs to know how to escalate that complaint.

Equally, if the complaint regards a specific agent, there also needs to be a process in place around agent discipline. In severe cases, if any agent has accessed a customer's accounts by stealing his or her PIN, often some mobile money operators will block the agent account immediately pending further investigation. For more minor offences at the agent level, operators will typically give an agent a warning before taking action.

When controls aren't an option: transfer, tolerate or terminate risks.

If a risk isn't acceptable, an operator may make a decision to transfer the risk. Insurance is one form of risk transfer, but the more relevant one for most mobile money operations is outsourcing. The use of third parties (such as agents, cash handling companies or business process operators) may reduce the risk for an operator. However, many regulations may stipulate that the bank or operator responsible cannot transfer some forms of liability.

UBL Omni: When to tolerate and when to control risks

In Pakistan, UBL, wanted to find ways to encourage its mobile money customers using Omni over-the-counter (OTC) to move to e-wallets. Due to amended regulation, UBL was able to allow new Omni customers to conduct two transactions prior to the account verification, allowing for certain transactions to be completed by SMS authentication. UBL decided to implement the new option as a way to reduce barriers for customers to trial the e-wallet.

The fraud and risk team recognised that there was an additional risk of fraudulent activity by allowing customers to transact under certain circumstances without a PIN. The team decided that the commercial benefit outweighed the risk and tolerated the risk at launch by allowing certain lower value transactions. They monitored the activity and within the first week, they discovered there were a few complaints from some customers. These customers complained that transactions had been completed from their accounts without their knowledge.

As a response, the fraud and risk team decided to implement an additional control. Within a week, they had restricted the allowable transactions such that disbursal codes were mandatory in lieu of a PIN.

UBL was able to tolerate the risk at launch because they knew they had the capabilities, due to their technology, to react quickly if the perceived risk impact increased. What is equally important is that while UBL decided to tolerate the risk, they closely monitored activity to ensure they were immediately aware of any impact.

Alternatively, there are cases where a deployment may choose to tolerate a risk. Sometimes a good option is to accept that a risk will occur since the cost-benefit analysis of preventing the risk indicates that the cost or customer impact is too high. If this decision is taken, it should be monitored closely in case the cost-benefit equation changes.

Terminating a risk is another possible route when a practical and effective control is not possible. If a particular product or service is creating many possibilities for loss or fraud, customer issues or other problems, the best option is sometimes to discontinue that product. It may be necessary to "grandfather" a particular pricing scheme or otherwise manage change for those affected.

Monitor and review risk Management strategy: ensuring long-term effectiveness

Monitoring the controls and reviewing the risks over time is crucial in maintaining an effective risk mitigation strategy in mobile money.

Questions to be addressed in the monitoring process

- What new fraudulent activities are happening? Is there a trend?
- Are all controls adequately designed and executed?
- Are employees and managers aware and understand their roles and responsibilities?

Monitoring requires strong management support and adequate internal resources

Firstly, it is important that the risk management process has detailed involvement of management. Many mobile money operators have a dedicated Risk Management Committee consisting of Senior Management from different parts of the business. This may also involve representation of the Board of Directors or banking partners. It should have a standing agenda to review the current risk profile, the effectiveness of controls and be on the lookout for any new or emerging risks. It may also have a role in the approval of new or changed products or services. Throughout the risk management process, it is important that management has validated the risk assessment and risk acceptance decisions.

One of the most common forms of monitoring used by mobile money deployments is an annual internal audit. This is a comprehensive review to ensure all processes and controls are performed in a timely manner and completed by a team that is not directly involved with the mobile money service. Often the internal audit team sits at the group level or may be part of the finance and revenue assurance team. Mobile money providers may rely on the same internal audit team that conducts the risk audit on the GSM side of the business. The latter option may be more attractive for smaller deployments due to the cost synergies. However, operators that use this approach need to ensure the GSM audit is appropriately adapted for mobile money.

Beyond the standard review of an internal audit, there are also more creative ways that we have seen mobile money deployments manage the monitoring process. WING in Cambodia monitors reconciliation via peer review. Reconciliation manipulation is arguably one of the highest risks in mobile money requiring a number of preventive and detective controls including clear segregation of duties and monitoring system access and activity. At WING, managers who are not directly involved in the process do the reconciliation as a random spot-check. There are two benefits to this process. First, managers become more familiar with the necessary steps to perform the reconciliation and therefore are more capable to identify if there any irregularities reported. Second, the manager acts as an outside monitor reducing the risk of collusion between those who regularly conduct the reconciliation.

Monitoring is critical to the success of risk management because mobile money deployments will evolve and with more product offerings or simply a growing customer base, controls will need to be reviewed to ensure on-going effectiveness. Equally important is that while the deployment changes, so too does the sophistication of fraudsters. Operators need to ensure adequate resources to regularly review both the effectiveness of controls and the market for potential new trends in fraudulent activity. Regular reviews coupled with active management involvement are both necessary for operators to ensure long-term sustainability of effective risk management.

Fraud and risk are key questions that must be addressed by any mobile money operator. They are the concern not only of the operator, but also the concern of the customers, the agents and the regulators. Our research has shown that there are many tactics that operators can use to identify, prioritise, control and monitor the risk of frauds. By ensuring that frauds are managed according to this framework, operators can protect themselves, their customers and agents and help contribute to a successful mobile money business.

BILL & MELINDA GATES foundation

The MasterCard Foundation

OMIDYAR NETWORK™

The MMU programme is supported by The Bill & Melinda Gates Foundation, The MasterCard Foundation, and Omidyar Network

For further information please contact
mmu@gsm.org
GSMA London Office
T +44 (0) 20 7356 0600
http://www.gsma.com/mmu