GSMA

Mobile Money Certification Guidance

GSMA™

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

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

We invite you to find out more at www.gsma.com

Follow the GSMA on X: @GSMA

GSMA Mobile Money

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

For more information, please contact us:

www.gsma.com/mobilemoney

X: @GSMAMobileMoney

mobilemoney@gsma.com

Published March 2024

GSMA

Contents

Background and context 05

Principle 1 Safeguarding of funds 06

Objective of the provider’s Safeguarding Policy & Procedures 07

Protection against loss due to failure of the bank, mobile money provider or third party 08

Objective of reconciling the safeguarding account 09

Dealing with reconciliation variances 10

Protection of funds against loss due to insolvency of the mobile money provider 11

Protection of funds against settlement risk 12

Principle 2 AML/CFT/fraud 13

Commitment to AML/CFT compliance 14

Principle 3 Staff and partner management 19

Objectives of staff and partner management 20

Due diligence policies and procedures 21

Development and implementation of training programmes for staff and agents 22

Contractual agreements 23

Management of staff, agents and entities providing outsourced services 24

Principle 4 Quality of operations 25

Objectives 26

Board and senior management oversight of the mobile money service 27

Business and technical operations and service-level management 28

Capacity Management 29

Incident & Problem Management 30

Change and configuration management 31

Enterprise risk management 32

Service Continuity And Contingency Plans 33

Principle 5 Security of systems 34

Objectives 35

Security governance 36

Designing and developing secure systems, applications and networks 37

Security operations 38

Principle 6 Transparency 39

Transparency of fees and terms and conditions 40

Educating customers about safety and security 42

Principle 7 Customer service 44

Key elements of a customer service policy 45

Complaints management process 46

Transaction reversals 48

Principle 8 Data privacy 49

Objective of a data privacy programme 50

PwC’s data privacy framework 51

The European Union’s GDPR 52

Data Protection Officer: job description and responsibilities 53

Annexes 56

Annex 1 Methodology 57

Annex 2 Recommended reading 58

Annex 3 Waiver of Liability 59

Background and context

The GSMA Mobile Money Certification was launched in 2018 to bring safer, more transparent, trusted and more resilient financial services to millions of mobile money users around the world. It does this by promoting excellence in the provision of mobile money services and setting a public bar to which all mobile money providers can aspire. The Certification is based on independent assessments of a mobile money provider's ability to deliver secure and reliable services, to protect the rights of consumers and to combat money laundering and the financing of terrorism in line with industry and global best practices.

Purpose of the guidance

The purpose of the GSMA Mobile Money Certification guidance is to:

1. Foster a common understanding among mobile money providers of what constitutes acceptable evidence of compliance for each principle of the GSMA Mobile Money Certification.
2. Set out key elements of acceptable evidence for Certification assessment.
3. Encourage mobile money providers in fragile and high-risk markets to use this guidance to assess their related[1] policies and procedures and make changes, as appropriate.

This guidance supplements the Mobile Money Certification Assessment Toolkit and should be read in conjunction with it.

Target audience

The target audience for this guidance is mobile money providers and other digital financial services (DFS) providers that intend to be assessed for the GSMA Mobile Money Certification.

[1] In line with the GSMA Mobile Money Certification principles.

Principle 1
Safeguarding of funds

Effective policies for the safeguarding of customer funds should include at least the following as evidence of compliance with Principle 1 of the GSMA Mobile Money Certification.

Objective of the provider's Safeguarding Policy & Procedures[2]

Principle 1 focuses on safeguarding customer funds. It emphasises the importance of implementing robust mechanisms to ensure customer funds are adequately protected, secure and available for use whenever they are needed. This principle encompasses various aspects, including risk management frameworks, compliance with regulatory requirements, secure technology infrastructure and mechanisms for handling customer funds in a transparent and accountable manner. By adhering to Principle 1, mobile money service providers demonstrate their commitment to maintaining the safety and integrity of their customers' financial resources, fostering trust and confidence in their services.

The following best practices have been adopted by a number of mobile money providers in Africa and Asia to satisfy the evidence requirement of the GSMA Mobile Money Certification.

> Compliance with Principle 1 helps to build trust and improve the reliability and credibility of mobile money services, fostering financial inclusion.

- The board of directors has signed off on the policy.
- The policy required the creation of a dedicated and independent finance unit, which is headed by a senior and qualified team member who reports directly to the CEO and the board, not to the Head of Finance.
- The unit is equipped with the necessary resources, including budgets, technology and human resources to achieve its objectives on a daily basis.
- The total value of outstanding mobile money liabilities should, ideally, be held in one or more custodial accounts on behalf of mobile money users.
- The custodial account should be held in a financial institution regulated by the central bank or equivalent regulatory authority.
- The team documents the custodial bank reconciliation process and performs, at least daily, reconciliations between the outstanding mobile money and total value of mobile money user funds held in custodial accounts.
- All transactions should be completed in real time, including multi-stage transactions (requiring third-party action before completion).
- The policy includes procedures for resolving reconciliation discrepancies promptly, including escalation steps.

[2] Financial Conduct Authority. (November 2021). "Chapter 10 – Safeguarding". *FCA Payment Services and Electronic Money – Our Approach. The FCA's role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011.*

Protection against loss due to failure of the bank, mobile money provider or third party

To protect client funds against losses that might incur due to either the failure of the bank where the funds are stored or the bankruptcy of the mobile money provider itself, providers should ensure that funds equal to the total value of outstanding mobile money liabilities are held in one or more custodial accounts on behalf of mobile money users. Providers must also ensure that user funds are ring-fenced to prevent their creditors from claiming them in the event of insolvency.

Under Principle 1 of the GSMA Mobile Money Certification, key evidence requirements for protection against loss due to the failure of banks, mobile money providers or other parties, might include:

- **Custodial accounts:** Client funds are held in an account separate from the mobile money provider's main trading account with a bank that is recognised and regulated by the national financial regulator.
- **Custodial account statements:** Documentation providing evidence of custodial account statements that demonstrate the separation of customer funds from operational funds.
- **Escrow agreements:** Records detailing escrow agreements or arrangements established to protect customer funds in case of mobile money provider or bank insolvency.
- **Insurance policies:** Evidence of insurance policies or indemnity arrangements safeguarding customer funds against potential loss due to insolvency or other failures.
- **Contingency plans:** Documentation outlining contingency plans developed to ensure access to customer funds in case of provider or bank failure, ensuring minimal disruption for users.
- **Regulatory compliance records:** Evidence showcasing compliance with regulations and standards ensuring protection against losses due to the failure of banks or mobile money providers.
- **Independent audits:** Reports from independent audits verifying the adequacy of measures in place to protect customer funds from losses due to failure of relevant parties.
- **Legal agreements:** Records of legal agreements or contracts outlining the responsibilities and obligations regarding the protection of customer funds in case of insolvency or failure.

These evidence requirements validate the implementation of measures and arrangements aimed at shielding customer funds from potential losses due to the failure of banks, mobile money providers or third parties, ensuring the security and protection of user funds within the mobile money ecosystem.

Objective of reconciling the safeguarding account[3]

The “balancing exercise”, commonly referred to as the “reconciliation exercise”, is the mechanism for ensuring the outstanding customer funds being held electronically are always backed by an equivalent physical amount stored securely in the safeguarding/custodial account. This provides users with assurance that their money is available and safe.

Based on our research, the following best practices should be applied to address the evidence requirement of the GSMA Mobile Money Certification:[4]

- Documentation detailing the procedures, protocols and frequency of reconciling the safeguarding account, demonstrating adherence to best practices.
- The bank reconciliation process should clearly specify the start and end point of each reconciliation period, clearly defining which transactions should be included to reach the final settlement position.
- A procedure should be specified for resolving reconciliation discrepancies.
- Records demonstrating regular reconciliations between e-money issued and funds held in custodial accounts, ensuring alignment and accuracy.
- The value of funds held across all custodial accounts must be equal to or greater than the total value of outstanding mobile money liabilities.
- A reconciliation with the custodial bank should be performed at least daily on weekdays.
- Furthermore, on days designated as bank holidays, an additional reconciliation should be performed at the start of the next working day to cater to transactions made during the bank holiday period.
- Reconciliation data should be transferred via direct data exchange between the systems of the mobile money provider and the custodial bank to reduce the risk of errors and fraud.
- Documentation outlining the audit trails and processes used to reconcile and verify the consistency of e-money issuance and funds in custodial accounts.

These evidence requirements validate the mobile money provider’s commitment to ensuring accuracy and alignment between the e-money issued and the funds held in custodial accounts. They ensure transparency, accuracy and reliability in managing customer funds within the mobile money ecosystem, fostering trust and confidence among users and stakeholders.

[3] ISO 27000:2018

[4] Financial Conduct Authority. (November 2021). *FCA Payment Services and Electronic Money – Our Approach. The FCA’s role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011*.

Dealing with reconciliation variances

An integral part of Principle 1, and overall policy, is having a system in place to help the mobile money finance operations team, which would be separate from the operations team, to deal with any variance between outstanding customer funds and the equivalent physical amount stored securely in the safeguarding/custodial accounts, if and when this happens.

As best practice, the following steps have been implemented by GSMA-certified mobile money providers:

- Documentation detailing instances of reconciliation variances or discrepancies between the mobile money issued and the funds held in custodial accounts.
- All variances are identified and understood.
- An action plan is in place for resolution, which is being followed and tracked by the Head of Finance.
- Efforts are made to promptly resolve each discrepancy.
- A monitoring plan is in place to deal with long-term issues.
- Efforts are made to understand the root causes of all discrepancies.
- One certified mobile money provider's policy indicated that if a variance is more than 5% of the sum value of the custodial bank accounts, it is to be treated as a top priority and will trigger an automated email to the CEO and board chair.
- If there is a recurring variance, further analysis must be carried out even though it may be less than 1% of the sum value of the custodial bank account(s) balances.

These evidence requirements validate a proactive approach to identifying, investigating and rectifying any discrepancies or variances that arise during reconciliations. They ensure the establishment of robust processes and controls to promptly address and resolve any inconsistencies between e-money issuance and the funds held in custodial accounts, maintaining accuracy and integrity in the management of customer funds.

Protection of funds against loss due to insolvency of the mobile money provider[5]

User funds must be legally segregated from the mobile money provider's assets to ensure these funds may not be claimed by their creditors in the event of insolvency.

Objective of protecting funds from mobile money provider insolvency

Segregating user funds in inaccessible accounts during insolvency shields individuals from losing their money in the event of a provider's collapse. This practice prioritises customer protection, ensuring their funds remain untouched and separate from the provider's assets. By safeguarding these funds from liquidation proceedings, it upholds trust in the service provider, encouraging user participation and confidence in the mobile money ecosystem. This approach aligns with regulatory standards, fortifying the integrity of financial systems, and assures users that their funds are secure – even amid the provider's financial challenges – fostering a resilient and secure financial environment for customers.

The above objective could only be achieved where funds are held in some form of a "trust" account that stipulates the funds are protected from the mobile money provider's creditors. In other words, funds held by the trust may not be claimed by the provider's creditors or the trustee's creditors.

Please be aware that in cases where regulatory limitations prevent full protection of user funds from the mobile money provider's creditors in the event of insolvency, this risk can be reduced if the provider ensures that contractual agreements with creditors acknowledge the ring-fencing and unavailability of these assets in such circumstances.

[5] FCA Handbook – CASS 7.13.12 and 7.1.3.13

Protection of funds against settlement risk

Protecting against settlement risks is crucial to ensure the stability and security of customer funds. Mitigating settlement risks prevents potential disruptions or losses in the settlement process, maintaining the integrity of transactions and safeguarding user funds. By implementing robust measures to counter settlement risks, such as secure custody arrangements, adherence to regulatory standards and contingency plans, mobile money providers can ensure the reliability and continuity of settlement processes, safeguarding customer funds against potential volatility or uncertainties in financial settlements.

Under Principle 1 of the GSMA Mobile Money Certification, key evidence requirements for protection against settlement risk might include:

- **Settlement procedures documentation:** Records outlining established settlement procedures, protocols and controls, ensuring accuracy and reliability in settlement processes.
- **Custodial account statements:** Documentation demonstrating segregation of customer funds in custodial accounts, separate from operational funds, to mitigate settlement risks.
- **Escrow agreements:** Evidence of escrow agreements or arrangements designed to mitigate settlement risks and ensure the availability of funds for settlement purposes.
- **Insurance policies:** Evidence of insurance policies or indemnity arrangements mitigating settlement risks, securing funds in case of settlement failures or disruptions.
- **Contingency plans:** Documentation outlining contingency plans developed to manage settlement risks, ensuring continuity and minimal disruption in settlement processes.
- **Standard transaction processing:** Evidence that all transactions are processed in real time, i.e., debits and credits are made on the mobile money platform at the same time.
- **Multi-party transaction processing:** Evidence to demonstrate that funds are debited or reserved from the sending party's account as soon as the transaction has been authorised by the mobile money sender.
- **Reconciliation and settlement process:** Records indicating a specific reconciliation and settlement process, where needed, is in place with applicable financial partners.
- **Compliance records:** Evidence showing compliance with regulatory requirements aimed at mitigating settlement risks and protecting customer funds during settlements.

These evidence requirements validate a mobile money provider's commitment to implementing measures and arrangements that mitigate settlement risks. They ensure the reliability, accuracy and security of settlement processes, safeguarding customer funds against potential volatility or uncertainties in settlement activities within the mobile money ecosystem.

Principle 2
AML/CFT/fraud

The objective of an anti-money laundering/combating the financing of terrorism (AML/CFT) compliance programme is to ensure that all financial crime risks, including money laundering and terrorist financing, are identified and appropriately addressed and mitigated to protect the mobile money provider and all internal and external stakeholders.

Commitment to AML/CFT compliance

To achieve the objective of an AML/CFT programme, senior management must demonstrate their commitment by setting up a dedicated compliance unit and allocating adequate resources to it.

Dedicated compliance unit

The compliance unit is responsible for the appointment of a Money Laundering Reporting Officer (MLRO), customer due diligence (CDD), monitoring and reporting of suspicious activities, AML and CFT training and managing fraud risks.

The following are key elements that mobile money providers in Asia have included in their respective AML/CFT policies:

- The policy on which the board of directors has signed off creates a dedicated compliance unit headed by a senior and qualified team member.
- The compliance unit is responsible for monitoring and mitigating the risks of financial crime, as well as ensuring compliance with national regulations and laws.
- The unit is equipped with the necessary resources, including budgets, technology and human resources, to achieve its objectives every year.

Appointment of a Money Laundering Reporting Officer

MLROs play important roles at mobile money providers, whether the provider operates under an MNO-led or bank-led regulatory model. To be effective in their role, MLROs must have the requisite skills and knowledge acquired from sufficient experience and training. Their skills and knowledge should be in line with the size of the mobile money provider and risk of harm. Note that staff who have only worked in a front-line role and have less training and experience usually do not have the skills or knowledge to serve as an MLRO.

The following are key responsibilities of MLROs that mobile money providers in Asia have included in their respective policies:

The MLRO is designated by the board of directors as the officer responsible for overseeing AML/CFT activities with sufficient authority, including appraising the board and senior management of AML/CFT compliance initiatives, any significant compliance deficiencies and the reporting of suspicious activity to the Financial Intelligence Unit (FIU) and law enforcement authorities.

Customer due diligence

Customer due diligence (CDD), or know your customer (KYC), is the process of collecting and evaluating relevant information about a customer or potential customer. CDD aims to uncover any potential risk to the mobile money provider of doing business with a specific individual or organisation by vetting the information from various sources.

There are many reasons why mobile money providers conduct CDD and commit time and effort to knowing their customers:

- To ensure they remain compliant with the national regulations and laws under which they operate
- To ensure the customer really is who they say they are
- To guard against fraudulent activity, such as identity fraud or impersonation
- To assist law enforcement in keeping the nation secure

The following is a useful example of a CDD process taken from the due diligence policy of a mobile money provider with a large footprint.

- The customer shall ensure that they have provided the necessary KYC documents to the provider as required by law prior to the activation of the mobile money account.
- The provider shall carry out the necessary due diligence. If satisfied with the sufficiency and validity of the KYC documents, the provider shall activate the mobile money account.
- If the customer fails to provide the necessary KYC documents, or fails to satisfy the minimum KYC requirements, the provider will refuse to activate the mobile money account and accordingly advise the customer of the decision.
- For the avoidance of doubt, the provider's refusal to activate the mobile money account shall neither confer on the customer any right to contest the provider's decision nor give rise to any legal claim against the provider.

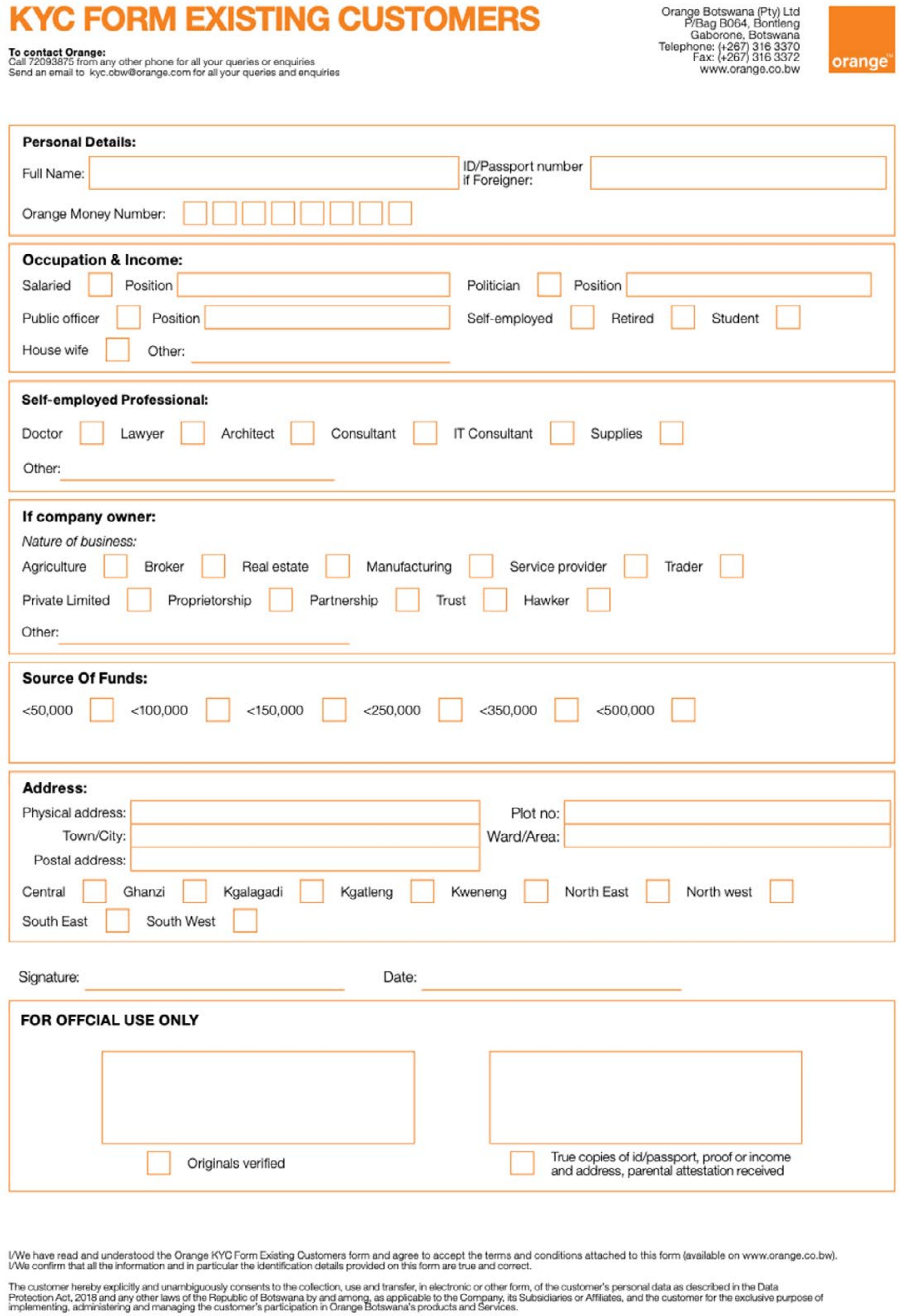
International standard-setting bodies (SSBs), such as the Financial Action Task Force (FATF), recommend a risk-based approach to implementing CDD protocols. The following is an example of an FATF-influenced CDD/KYC policy of a bank-led mobile money provider operating in a multi-jurisdictional environment.

Our KYC process starts at the time of onboarding the customers and runs at regular intervals throughout the customer lifecycle. The policy requires different levels of KYC based on the risks posed by the customer. For low-risk customers, name, address and date of birth are sufficient to open an account. For medium-risk customers, verification of this information is required and, for high-risk customers, proof of source of funds may also be required if the transaction value is large or exceeds a cumulative monthly figure.

Depending on the national regulations, biometric verification may be required in certain operating countries and so, as a group, compliance with KYC requirements vary among different operating companies.

In addition, international and domestic sanctions checks must be carried out for all account holders at the time of registration and thereafter every 12 months or as required by the regulations.

It is also important to document the data collected for KYC purposes. It is to be noted that the data collected should be free from all sorts of bias. Best practices indicate that a standard form should be used for KYC data collection and verification as per KYC regulations. A good example of KYC data collection is Orange Botswana's KYC form.



KYC FORM EXISTING CUSTOMERS

To contact Orange:
Call 72093875 from any other phone for all your queries or enquiries
Send an email to kyc.obw@orange.com for all your queries and enquiries

Orange Botswana (Pty) Ltd
P/Bag B064, Bontleng
Gaborone, Botswana
Telephone: (+267) 316 3370
Fax: (+267) 316 3372
www.orange.co.bw

orange™

Personal Details:

Full Name: ______ ID/Passport number if Foreigner: ______

Orange Money Number: □□□□□□□□

Occupation & Income:

Salaried □ Position ______ Politician □ Position ______

Public officer □ Position ______ Self-employed □ Retired □ Student □

House wife □ Other: ______

Self-employed Professional:

Doctor □ Lawyer □ Architect □ Consultant □ IT Consultant □ Supplies □

Other: ______

If company owner:

Nature of business:

Agriculture □ Broker □ Real estate □ Manufacturing □ Service provider □ Trader □

Private Limited □ Proprietorship □ Partnership □ Trust □ Hawker □

Other: ______

Source Of Funds:

<50,000 □ <100,000 □ <150,000 □ <250,000 □ <350,000 □ <500,000 □

Address:

Physical address: ______ Plot no: ______

Town/City: ______ Ward/Area: ______

Postal address: ______

Central □ Ghanzi □ Kgalagadi □ Kgatleng □ Kweneng □ North East □ North west □

South East □ South West □

Signature: ______ Date: ______

FOR OFFCIAL USE ONLY

□ Originals verified

□ True copies of id/passport, proof or income and address, parental attestation received

I/We have read and understood the Orange KYC Form Existing Customers form and agree to accept the terms and conditions attached to this form (available on www.orange.co.bw).
I/We confirm that all the information and in particular the identification details provided on this form are true and correct.

The customer hereby explicitly and unambiguously consents to the collection, use and transfer, in electronic or other form, of the customer's personal data as described in the Data Protection Act, 2018 and any other laws of the Republic of Botswana by and among, as applicable to the Company, its Subsidiaries or Affiliates, and the customer for the exclusive purpose of implementing, administering and managing the customer's participation in Orange Botswana's products and Services.

Monitoring and reporting of suspicious activities

One of the key roles of an MLRO is to monitor mobile money transactions and report suspicious ones to law enforcement agencies and the FIU of the regulator to mitigate financial crime risks. Monitoring is recommended using artificial intelligence (AI) or other algorithmic programmes or software that can analyse big data, as it is more efficient than human capabilities. Red flags that are raised should be assessed by the compliance function and the MLRO, and then the transaction should be processed according to the protocols implemented.

Financial crime risks are dynamic. Therefore, the required capabilities of MLROs and the intensity of monitoring may vary from one region or country to another. However, the basic activities, processes and capabilities are constant. The following excerpt provides an overview of the key responsibilities, as good practices, that a mobile money provider in Africa has included in their monitoring and reporting controls policy.

- As per the policy, all transactions are monitored for suspicious activities and behaviours through an automated, AI/algorithm-based programme that works round the clock.
- All red flags or alerts raised by the computer programme are monitored and assessed in real time by a dedicated compliance unit and transactions are held until investigations are complete but without tipping off.
- Suspicious transactions are then reported to the MLRO, who subsequently reports them to the regulator, law enforcement agencies and any other entities required by law.
- The policy requires immediate blocking of all mobile money accounts of customers that violate the terms and conditions, as well as those that have been blacklisted under the sanctions or AML/CFT monitoring. Such accounts must be reported to law enforcement agencies within 24 hours and barred from opening new accounts until the matter is legally resolved.

AML and CFT Training

A mobile money provider must take reasonable care to provide appropriate AML/CFT training to their staff, agents and distributors who handle, or are managerially responsible for the handling of, transactions that may involve such risks.

Since AML and CFT risks vary across jurisdictions, it is often difficult to establish common ground among providers on what constitutes a minimal acceptable level of training. Therefore, information from research conducted with mobile money providers is not highlighted here. Instead, we have considered guidance from SSBs such as the FATF. Based on this, the following crucial elements should be part of the AML and CFT training programme.

- AML/CFT laws and regulations
- Overview of the money laundering (ML) and terrorist financing (TF) risks, as well as common frauds that have a profound impact on the consumers and businesses in the jurisdiction
- Overview of the KYC and account registration protocols
- Overview of the provider’s risk management protocols and tools available, including reporting of identified risks
- Detailed awareness of the responsibilities of agents and staff in mitigating ML and TF risks
- Obligation of the super agent to train their staff on similar principles
- Overview of the whistle-blower programme
- Penalties for improper conduct
- Post-training assessment pass criteria

Fraud management

In 2020, an estimated USD 4 billion[6] was lost in mobile money frauds and scams. This presents a significant risk to users. Active fraud management is no longer just important, but a necessity. As the scope of mobile money services expand, fraud will become more prominent and profound. It is important to implement strong fraud management practices that include advanced analytical programmes – ideally AI-based – to detect and report fraud. While the technical aspects are covered in Principle 5 of the GSMA Mobile Money Certification, this principle focuses on the strengths of a fraud management policy.

The following excerpt is from a robust fraud management policy developed by a mobile money provider in Africa. It serves as a strong reference for providers in any region developing a fraud management policy and highlights the key aspects that should be covered.

- The purpose of the policy is to ensure that all staff, agents, business partners and other stakeholders are aware of their obligation to report suspected fraud (dishonesty, financial malpractice, illegal or criminal activity and breaches of business practices, among others).
- Deliberate failure to report could lead to disciplinary action.
- Policy includes a protection mechanism for whistle-blowers who do so in good faith.
- Provider will treat all such reports in a confidential and sensitive manner. The identity of the individual making the report shall be kept confidential unless required by law.
- For transparency, a reporting structure should be clearly stated. For example, this should include the Head of Ethics as the first line of reporting, CEO as the second and board of directors the third.
- Contact details should be included to report fraud. Ideally, a phone number, email address, web form and postal address should be included.

[6] Fitzhenry, W. (18 January 2022). “Visualizing a timeline of mobile money fraud”. *Cambridge Intelligence Blog*.

Principle 3
Staff and partner management

Under Principle 3 of the GSMA Mobile Money Certification, the management of staff, agents and third-party contractors encompasses key objectives vital to ensuring the efficiency and integrity of mobile money services.

Objectives of staff and partner management

The first objective emphasises due diligence and training of staff, ensuring their competency, ethical conduct and adherence to regulatory standards. This objective aims to establish a knowledgeable and compliant workforce capable of delivering quality service while mitigating risks associated with misconduct or non-compliance.

Second, managing agents involves stringent selection criteria, comprehensive training and ongoing performance monitoring. Agents serve as crucial touchpoints for users, which makes proper selection vital. Ensuring agents possess the necessary skills, comply with regulations and maintain service quality bolsters user trust in, and access to, the mobile money service.

Lastly, overseeing third-party contractors requires establishing clear agreements, outlining responsibilities, standards and compliance measures. This objective ensures that outsourced entities meet predefined criteria and contribute to the reliability and compliance of the service.

These objectives collectively fortify the mobile money ecosystem, fostering a competent workforce, reliable agents and accountable outsourced partners, essential for sustained service quality and user trust in the mobile money ecosystem.

Principle 3 of the GSMA Mobile Money Certification centres on effective management of staff, agents and outsourced service partners. It prioritises due diligence, comprehensive training and ongoing oversight of personnel to ensure compliance and competence. This principle aims to establish a robust network of knowledgeable agents, guided by stringent selection criteria and continuous support. Additionally, it emphasises clear agreements and oversight of third-party entities, fostering reliability and compliance within the mobile money ecosystem. Overall, Principle 3 focuses on cultivating a skilled workforce, reliable agents and accountable partners to ensure the integrity and efficiency of mobile money services.

Due diligence policies and procedures

Performing due diligence on staff, agents and service partners before and during their tenure is crucial for several reasons. It ensures the integrity of the mobile money ecosystem by mitigating risks associated with potential fraud, misconduct or non-compliance. Screening before employment safeguards against hiring individuals with dubious backgrounds and helps maintain the credibility of the system. Regular assessments align with evolving risks, maintaining a vigilant stance against vulnerabilities. This process upholds regulatory compliance, safeguards customer trust and ensures a robust, ethical and secure environment, crucial for sustaining the reliability and integrity of mobile money services.

The following best practices have been adopted by a number of mobile money providers in Africa and Asia.

- **Policy and procedures manual:** Documentation of staff and agent recruitment and the supplier onboarding due diligence process, which is regularly reviewed and updated as needed.
- **Staff due diligence records:** Documentation of identity documents (ID) and address verification checks, pre-employment background checks, qualifications and ongoing training records ensuring staff competence and compliance.
- **Agent selection criteria documentation:** Evidence of criteria used for selecting and onboarding agents, verifying suitability, reliability and adherence to standards. This would include ID and address verification of all owners (>25% ownership) and senior management of master agents/agent aggregator.
- **Agent training records:** Documentation showcasing training programmes provided to agents, ensuring they possess the skills for service delivery, compliance and technology use.
- **Performance monitoring reports:** Records indicating systems used to monitor and assess agent performance, ensuring quality service provision and compliance.
- **Compliance documentation:** Evidence demonstrating agents' and service partners' adherence to regulatory requirements, ensuring trust and credibility in the service.
- **Technology infrastructure proof:** Documentation showcasing agents' access to necessary technological tools and infrastructure for seamless transactions.
- **Fraud prevention measures:** Evidence of implemented measures to prevent fraud within the agent network, safeguarding users and the system.
- **Outsourced service partner agreements:** Evidence of contracts or agreements outlining responsibilities, standards and compliance measures for outsourced service partners.

The above evidence requirements serve to validate that staff, agents and outsourced partners comply with standards, undergo necessary training and contribute to a secure and reliable mobile money ecosystem.

Development and implementation of training programmes for staff and agents

Developing and implementing training programmes for staff and agents within Principle 3 of the GSMA Mobile Money Certification is crucial. They ensure that personnel possess the necessary skills, understanding of compliance and technical proficiency essential for seamless service delivery. Training instils best practices, mitigates risks and fosters a culture of compliance, enabling staff and agents to navigate evolving challenges effectively. It also enhances customer service quality, boosts confidence in the mobile money service and aligns operations with regulatory standards. Ultimately, robust training programmes empower staff and agents to uphold integrity, reliability and security within the mobile money ecosystem.

The following best practices have been adopted by other mobile money providers and could be used as a guide.

- **Training manual documentation:** Prepare detailed documentation outlining the curriculum and topics covered in the training programmes for staff and agents.
- **Training materials:** Keep copies of training materials, presentations, manuals or modules used during the training sessions.
- **Training attendance records:** Keep records indicating attendance and participation of staff and agents in the training programmes.
- **Assessment records:** Documentation showing evaluations or assessments conducted to measure the understanding and proficiency of staff and agents post-training.
- **Training effectiveness reports:** Reports demonstrating the effectiveness of the training programmes in enhancing skills, understanding of compliance and technical proficiency among staff and agents.
- **Feedback and improvement plans:** Documentation of feedback collected from staff and agents about the training programmes and any subsequent improvement plans based on feedback.

The above evidence requirements validate the comprehensive development, execution and impact of training initiatives, ensuring that staff and agents are equipped with the necessary knowledge and skills to perform their roles effectively within the mobile money ecosystem.

Contractual agreements

Written agreements governing relationships with agents and outsourced service entities under Principle 3 of the GSMA Mobile Money Certification outline roles, responsibilities, compliance standards and service expectations, ensuring clarity and alignment between the mobile money provider and these external entities.

Well-defined agreements play a crucial role in mitigating operational risks, setting performance metrics and establishing accountability, thereby fostering a transparent and mutually beneficial partnership. They serve as a safeguard against potential disputes, regulatory non-compliance or misunderstandings, ensuring the integrity of the mobile money service.

Additionally, these agreements enable a consistent and standardised approach to service delivery, promoting reliability, trust and adherence to regulatory guidelines.

Under Principle 3 of the GSMA Mobile Money Certification, key evidence requirements for written agreements governing relationships with agents and outsourced service entities include:

- **Signed agreements:** Keep copies of signed written agreements between the mobile money provider and agents or outsourced service entities, outlining roles, responsibilities and obligations.
- **Agreement terms and conditions:** Documentation detailing the terms, conditions and scope of the relationship between the mobile money provider and agents or outsourced service entities.
- **Compliance documentation:** Evidence demonstrating that the agreements align with regulatory requirements and industry standards.
- **Record of amendments or updates:** Documentation showcasing any amendments or updates made to the agreements over time, ensuring they remain current and relevant.
- **Confirmation of understanding:** Records indicating that all involved parties have understood and agreed to the terms outlined in the agreements.
- **Agreement review process:** Documentation of the review process for these agreements to ensure they are assessed periodically and updated as necessary.

These evidence requirements validate the existence, validity, compliance and ongoing relevance of written agreements, ensuring clear guidelines and expectations within relationships involving agents and outsourced service entities in the mobile money ecosystem.

Management of staff, agents and entities providing outsourced services

Effective management ensures adherence to standards, regulatory compliance and quality service delivery. Oversight of staff guarantees their competence, ethical conduct and ongoing compliance training, fostering a culture of accountability.[7]

Managing agents involves selection based on stringent criteria, continuous training and performance monitoring to ensure reliable service provision and fraud prevention. Similarly, overseeing outsourced entities ensures they meet agreed-upon standards, maintaining service quality and compliance.

This management framework fortifies the mobile money ecosystem, instilling reliability, security and confidence for users, regulators and stakeholders while upholding the credibility of the industry and fostering financial inclusion.

Under Principle 3 of the GSMA Mobile Money Certification, key evidence requirements related to the management of staff, agents and entities providing outsourced services include:

- **Human resources manual:** Evidence showing an implemented human resources policy that, among other things, determines how the provider will ensure there are appropriate human resources to implement and maintain the mobile money service. The policy should cover how to train and make staff aware of tipping off and whistle-blower requirements. The policy should be kept up to date and revised at least every two years.
- **Performance monitoring reports:** Records indicating systems used to monitor and assess staff performance, ensuring adherence to standards and quality service delivery.
- **Agent management documentation:** Evidence demonstrating criteria used for agent selection, training programmes and mechanisms for performance monitoring and compliance adherence. The performance monitoring should include a process for on-site visits and mystery shopping.
- **Outsourced service partner management:** Documentation outlining the criteria for selecting and managing outsourced service partners, including agreements, performance assessments and compliance checks.
- **Complaints procedure:** Evidence that action has been taken against agents who are the subject of customer complaints, including termination of regularly offending agents.
- **Improvement plans:** Documentation highlighting any identified areas of improvement or corrective actions taken based on performance assessments or audits.

These evidence requirements validate effective management practices, ensuring that staff, agents and outsourced partners comply with standards, are adequately trained and contribute to a secure and reliable mobile money ecosystem.

[7] ISO 20000-1:2018 Sec. 5.2

Principle 4
Quality of operations

Principle 4 of the GSMA Mobile Money Certification centres on operating the service well and reliably, encompassing several key objectives crucial for ensuring the dependability and efficiency of mobile money services. Primarily, it ensures that the Board of Directors and senior management establish effective management oversight of the Mobile Money Service.

Objectives

The focus should be on upholding certain service levels through the management of technical and business operations in accordance with agreed-upon standards. The operations manual should include specific measures that are implemented to continuously improve services based on user feedback and technological advancements. Additionally, robust contingency plans and disaster recovery mechanisms should be in place to minimise service disruptions in the event of unforeseen circumstances.

Another critical objective is transaction security, which prioritises the implementation of stringent security measures. Ensuring the confidentiality, integrity and authenticity of transactions safeguards against fraud, cyberthreats and unauthorised access. This objective is fundamental for fostering user trust and maintaining the credibility of the mobile money service.

Another important aspect of Principle 4 is enterprise risk management (ERM), with mobile money providers establishing a risk management framework (RMF) for identifying, assessing and controlling risks.

Furthermore, the principle underscores system reliability for handling transactions promptly and accurately, from preparing capacity management plans to maintaining a reliable technical infrastructure. It involves continuous monitoring, performance assessments and infrastructure upgrades to guarantee a seamless user experience.

Principle 4 of the GSMA Mobile Money Certification prioritises operating a dependable and secure service. It emphasises ensuring service availability, robust transaction security and reliable system performance. The principle underscores the need for a resilient technical infrastructure capable of handling transaction volumes efficiently. By focusing on these aspects, Principle 4 aims to guarantee uninterrupted service access, protect transactions from threats and maintain a reliable system, contributing to a trustworthy and dependable mobile money service for users.

Board and senior management oversight of the mobile money service[8,9]

Board and senior management oversight under Principle 4 of the GSMA Mobile Money Certification is pivotal since their involvement ensures strategic alignment, effective decision-making and robust governance frameworks for the mobile money service. Their guidance shapes policies, risk management strategies and compliance measures, aligning operations with industry standards and regulatory requirements.

Board oversight ensures accountability, transparency and responsible stewardship of user funds and data, fostering user trust. Moreover, their strategic vision facilitates innovation, scalability and continuous improvement, ensuring the service remains reliable, secure and adaptable to evolving market needs. Board and senior management stand as guardians, with their oversight ensuring reliability, resilience and ethical conduct of the service, crucial for sustaining user confidence, industry credibility and long-term success.

Under Principle 4 of the GSMA Mobile Money Certification, key evidence requirements for board and senior management oversight of a mobile money service include:

- **Strategic plans:** Documents outlining strategic plans developed by the board or senior management concerning the direction and objectives of the mobile money service.
- **Communication and review:** Strategic plan needs to be communicated to mobile money staff and should be reviewed and updated regularly, when necessary.
- **Board and senior management meeting minutes:** Records demonstrating discussions and decisions related to mobile money service oversight during board meetings.
- **Board policies and directives:** Documentation outlining policies, directives or resolutions specifically addressing mobile money service oversight.
- **Management reports:** Reports submitted by senior management to the board regarding the performance, risks and compliance of the mobile money service.
- **Audit reports:** Internal or external audit reports assessing the effectiveness of oversight mechanisms and compliance with regulations.
- **Risk management framework:** Documentation of risk management strategies and frameworks specifically designed for the mobile money service, approved by the board.
- **Compliance records:** Records indicating adherence to regulatory standards and industry best practices as overseen by the board or senior management.
- **Training and development programmes:** Documentation outlining training or development initiatives for board members and senior management related to mobile money service oversight.

These evidence requirements validate effective oversight, governance and decision-making by the board and senior management concerning the mobile money service, ensuring compliance, risk management and strategic direction.

[8] ISO 20000-1:2018 Sec 5.1

[9] ISO 20000-2:2019 Sec 9.2 and Sec 9.2.2

Business and technical operations and service-level management[10,11]

Having robust business and technical operations alongside service-level management ensures operational efficiency and service reliability. Principle 4 of the GSMA Mobile Money Certification establishes streamlined processes, optimal system performance and adherence to predefined service standards.

Business and technical operations management ensures transactions are handled smoothly, risks are mitigated and user trust is maintained. Service-level management guarantees consistent service quality, timely resolution of issues and user satisfaction. This comprehensive approach fosters a dependable and efficient mobile money service, meeting user expectations while upholding industry standards, crucial for sustained growth and user confidence in the service.

Under Principle 4 of the GSMA Mobile Money Certification, key evidence provided by certified providers includes:

- **Operating procedures documentation:** Detailed documentation outlining operational procedures, workflows and protocols for mobile money service operations.
- **Back-up procedures:** Detailed documentation, either as part of the operating procedures or separately, outlining the frequency, mechanism and location of back-up storage together with the data retention period.
- **System performance reports:** Records demonstrating the performance metrics and benchmarks for the technical infrastructure supporting the mobile money service.
- **Incident response and resolution records:** Documentation detailing the procedures and timelines for incident response and issue resolution related to the service.
- **Service-level agreements (SLAs):** Agreements outlining the agreed-upon service levels, response times and performance benchmarks for the mobile money service.
- **User feedback and complaints records:** Documentation of user feedback, complaints and resolutions, demonstrating service responsiveness and adherence to service levels.
- **Change management documentation:** Records outlining procedures for implementing changes or updates to the mobile money service, ensuring minimal disruptions and adherence to standards.
- **Audit reports:** Internal or external audit reports assessing the effectiveness of business and technical operations and adherence to SLAs.

These evidence requirements validate the efficiency, reliability and compliance of business and technical operations, ensuring service-level management aligns with predefined standards and user expectations within the mobile money ecosystem.

[10] ISO 20000-1:2018 Sec 6.3

[11] ISO 20000-1:2018 Sec 9.3

Capacity Management[12,13]

The objective of implementing capacity management within Principle 4 of the GSMA Mobile Money Certification is to ensure the scalability and resilience of the mobile money service. It anticipates and meets user demands while maintaining system performance.

Capacity management plans accommodate growth, preventing service disruptions during peak usage, ensuring a seamless and reliable user experience. They enable proactive resource allocation, optimising infrastructure to handle transaction volumes and guarantee that the service remains robust, adaptable and capable of accommodating changing user needs and market dynamics.

Under Principle 4 of the GSMA Mobile Money Certification, key evidence requirements for capacity management typically include:

- **Capacity planning documentation:** Records outlining the methodologies and processes used for forecasting and planning for future user demands and transaction volumes.
- **Infrastructure scaling strategies:** Documentation showcasing strategies for scaling technical infrastructure (servers, networks, etc.) to accommodate increased user loads and transaction volumes.
- **Performance testing reports:** Records indicating the results of performance tests conducted to assess the system's capacity to handle projected transaction volumes.
- **Resource allocation plans:** Documentation outlining plans for allocating resources (hardware, software, personnel) to support increased service capacity.
- **Incident response and recovery plans:** Plans detailing responses to capacity-related incidents, ensuring minimal service disruptions during high-demand periods.
- **Monitoring and reporting mechanisms:** Records indicating systems used to continuously monitor system capacity and performance against established thresholds.
- **Review and improvement records:** Documentation showcasing reviews of capacity management strategies and any subsequent improvements made based on performance evaluations or market changes.

These evidence requirements validate a proactive approach to capacity management, ensuring the service remains scalable, resilient and capable of handling varying transaction volumes and user demands effectively.

[12] ISO 20000-1:2019 Sec 6.2

[13] ISO 20000-1:2019 Sec 8.4.3

Incident & Problem Management[14,15]

Incident and problem management within Principle 4 of the GSMA Mobile Money Certification ensures swift resolution of service disruptions and identifies underlying issues to prevent them from recurring. It minimises downtime, preserving user trust by promptly addressing issues affecting service reliability.

Incident management handles immediate disruptions, restoring service efficiently. Problem management investigates root causes, implementing preventive measures for long-term service stability.

This proactive approach maintains operational efficiency, mitigates risks and upholds service quality, vital for sustaining user confidence and ensuring a dependable mobile money ecosystem.

Under Principle 4 of the GSMA Mobile Money Certification, key evidence requirements for incident and problem management typically include:

- **Incident reports:** Documentation detailing incidents, their impact, steps taken for resolution and the time taken to restore service.
- **Problem root cause analysis:** Records demonstrating the investigation into the root causes of recurring incidents and actions taken to address these underlying issues.
- **Resolution timeframes:** Records indicating the time taken to resolve incidents and problems, ensuring adherence to predefined SLAs.
- **Incident and problem escalation procedures:** Documentation outlining procedures for escalating critical incidents or problems to higher management or specialised teams.
- **Incident response plans:** Documentation detailing predefined responses to different types of incidents, ensuring swift and effective action.
- **Continuous improvement records:** Documentation showcasing improvements made to prevent recurrence of incidents or problems based on post-incident evaluations.
- **Training and awareness programmes:** Records outlining training sessions or awareness programmes conducted for staff involved in incident and problem management.

These evidence requirements validate a structured approach to incident resolution, problem analysis and continuous improvement, ensuring a resilient and reliable mobile money service.

[14] ISO 20000-1:2019 Sec 8.6.1
[15] ISO 20000-1:2019 Sec 8.6.3

Change and configuration management[16,17,18,19]

Within Principle 4 of the GSMA Mobile Money Certification, change and configuration management ensure controlled modifications to the mobile money service, overseeing alterations to software, hardware and configurations. This systematic approach minimises the risks of service disruptions by assessing and implementing changes through change management, which maintains service reliability. Concurrently, configuration management tracks system components to ensure consistency and accurate documentation. This structured process not only safeguards against unauthorised changes, but also upholds service stability and guarantees seamless transitions. These aspects are vital for sustaining a secure and dependable mobile money ecosystem, ensuring it is resilient and reliable.

Under Principle 4 of the GSMA Mobile Money Certification, key evidence requirements for change and configuration management typically include:

- **Change requests and approvals:** Documentation showcasing requests for system changes, detailing the nature of changes and approvals obtained before implementation.
- **Change implementation records:** Records indicating the execution of approved changes, outlining the steps taken and any associated tests or validations performed.
- **Change impact assessment:** Documentation demonstrating assessments of the potential impacts of proposed changes to the mobile money service.
- **Configuration management database (CMDB):** Records depicting the CMDB, outlining the components, versions and relationships within the technical infrastructure of the mobile money service.
- **Configuration baselines:** Documentation outlining baseline configurations for different system components, serving as a reference for changes and ensuring consistency.
- **Change control procedures:** Documentation detailing procedures for controlling and managing changes, ensuring adherence to predefined policies and minimising risks.
- **Version control records:** Records indicating the versions of software or systems implemented, helping to track changes and manage configurations effectively.

These evidence requirements validate a structured and controlled approach by the mobile money provider to manage changes and configurations within the service, ensuring reliability, consistency and security.

[16] ISO 20000-1:2019 Sec 8.5
[17] ISO 20000-1:2019 Sec 8.5.2
[18] ISO 20000-1:2019 Sec 8.5.3
[19] ISO 27002: 2022

Enterprise risk management[20,21,22,23,24]

Enterprise risk management (ERM) within Principle 4 of the GSMA Mobile Money Certification systematically identifies, assesses and mitigates potential risks across operations, technology and compliance.

ERM ensures proactive risk mitigation, enhancing service resilience against threats like fraud, cybersecurity breaches or regulatory noncompliance.

This structured approach fortifies the mobile money ecosystem, safeguarding user trust, operational continuity and regulatory adherence. ERM cultivates a culture of risk awareness and enabling swift responses to emerging risks, crucial for sustaining a secure, dependable and compliant mobile money service in an ever-changing landscape.

Under Principle 4 of the GSMA Mobile Money Certification, key evidence requirements for ERM typically include:

- **Risk management policies and procedures:** Documentation outlining policies and procedures governing ERM practices within the mobile money provider's operations. The document/ policy should include the scope, process, governance and organisational structure.
- **Change requests and risk assessment documentation:** Records demonstrating comprehensive assessments of risks across various aspects of mobile money operations, technology and compliance.
- **Risk mitigation plans:** Documentation outlining strategies and plans for mitigating identified risks, including preventive measures and contingency plans.
- **Risk register:** A comprehensive register listing identified risks, their likelihood, potential impact and planned mitigation actions.
- **Risk monitoring reports:** Records indicating ongoing monitoring and evaluation of risks, including updates to the risk register based on changes in the risk landscape.
- **Incident and issue logs:** Records documenting incidents, issues or breaches related to risks and the actions taken for resolution or mitigation.
- **Compliance adherence reports:** Documentation showcasing adherence to regulatory requirements and industry standards concerning risk management.

These evidence requirements validate the mobile money provider's structured approach towards identifying, assessing, mitigating, and monitoring risks, ensuring a resilient and secure mobile money service.

[20] ISO 27005:2018 Sec. 7.1
[21] ISO 27005:2018 Sec. 8 and 12.1
[22] ISO 27005:2018 Sec. 7 and 7.2.3
[23] ISO 27005:2018 Sec. 9
[24] ISO 27005:2018 Sec. 11

Service Continuity And Contingency Plans[25,26,27,28,29]

Service continuity and contingency plans under Principle 4 of the GSMA Mobile Money Certification act as a safeguard mechanism for mobile money providers. They ensure seamless operations during unforeseen disruptions or disasters, maintaining service availability and minimising downtime. These plans outline strategies to mitigate risks, recover operations swiftly and ensure uninterrupted service delivery.

By preparing for scenarios like system failures, natural disasters or cyberincidents, these plans bolster the resilience of the service, ensuring user trust, regulatory compliance and operational continuity, critical for a dependable and secure mobile money ecosystem in the face of unforeseen challenges.

The following key requirements are based on best practices adopted by various mobile money providers:

- **Business continuity plans (BCPs):** Documentation outlining strategies and procedures to ensure continued service delivery during disruptions or emergencies.
- **Disaster recovery plans (DRPs):** Records detailing processes and actions to recover and restore operations following a catastrophic event or system failure.
- **Test and exercise records:** Documentation demonstrating tests, simulations or drills conducted to evaluate the effectiveness of contingency plans.
- **Incident response plans:** Plans outlining steps and procedures to address specific incidents, ensuring minimal service disruption and swift resolution.
- **Communication plans:** Documentation outlining communication strategies during emergencies, ensuring stakeholders are informed and updated.
- **Plan updates:** Records indicating periodic reviews, updates or revisions made to the contingency plans based on evaluations or changes in risk landscapes.
- **Training and awareness programmes:** Records showcasing training sessions or programmes conducted to educate staff on contingency procedures and their roles during emergencies.

These evidence requirements validate a mobile money provider’s preparedness, resilience and capability to maintain service continuity and respond effectively during emergencies or disruptions, ensuring a dependable and secure mobile money service.

[25] ISO 22313:2020 Sec. 5.2 and 5.3
[26] ISO 22313:2020 Sec. 8.2.2 and 8.2.3
[27] ISO 22313:2020 Sec. 8.3 and 8.4
[28] ISO 22313:2020 Sec. 8.5, 9.1 and 9.3
[29] ISO 22313:2020 Sec. 8.5 and 9.10

Principle 5

Security of systems

Principle 5 of the GSMA Mobile Money Certification focuses on protecting a mobile money provider's system through robust cybersecurity measures, compliance with standards and fostering a security-conscious culture within the organisation.

Objectives

The first main objective under Principle 5 is establishing robust security governance frameworks. This includes defining clear security policies, assigning responsibilities and establishing accountability for security-related matters. Objectives also encompass periodic risk assessments, ensuring ongoing evaluations of potential threats and implementing measures to address these risks. Moreover, the objective aims to promote a culture of security awareness and compliance within the organisation, fostering a vigilant workforce.

The second main objective is to ensure a secure system, applications and network design and development. Objectives include implementing robust security measures during system architecture, coding and network configuration phases. This involves incorporating encryption, access controls and secure coding practices to mitigate vulnerabilities. Additionally, the objective emphasises regular security testing and audits to identify and rectify potential weaknesses. The primary aim is to create resilient and secure infrastructure that protects against cyberthreats, safeguards user data and ensures the integrity and confidentiality of mobile money services, enhancing overall system security.

The final main objective is effective security operations. This includes establishing robust incident response procedures, promptly addressing security breaches and ensuring potential threats are continuously monitored. This involves deploying security incident and event management (SIEM) systems, conducting regular security audits and maintaining incident response readiness. Additionally, the objective emphasises the implementation of intrusion detection systems and regular security updates. By prioritising security operations, Principle 5 aims to swiftly detect, respond to and mitigate security incidents, ensuring the ongoing integrity and resilience of the mobile money service.

> By prioritising security governance, designing and developing secure systems and applications, and by managing effective security operations, Principle 5 seeks to maintain a secure and resilient mobile money service.

Security governance[30,31,32,33,34]

Security governance under Principle 5 of the GSMA Mobile Money Certification is vital to maintaining a robust security framework. It establishes clear policies, delineates responsibilities and defines accountability for security-related matters within the organisation. This governance structure ensures consistent adherence to security protocols, enabling proactive risk assessment and mitigation. By fostering a culture of compliance and vigilance, security governance mitigates threats, maintains regulatory adherence and fortifies the mobile money ecosystem against cyber-risks.

Under Principle 5 of the GSMA Mobile Money Certification, key evidence requirements for security governance typically include:

- **Security policies and procedures:** Documentation outlining comprehensive security policies, protocols and procedures established within the organisation.
- **Roles and responsibilities:** Records delineating specific responsibilities and accountabilities for security-related tasks and roles within the organisation.
- **Risk management plans:** Documentation showcasing periodic risk assessments and identification of threats and strategies to mitigate potential risks.
- **Compliance records:** Evidence demonstrating compliance with security standards, regulations and industry best practices.
- **Security governance framework:** Records outlining the structured framework or guidelines governing security practices and decision-making processes.
- **Incident response plans:** Documentation detailing protocols and procedures for addressing security incidents, ensuring a swift and effective response.
- **Training and awareness programmes:** Records indicating security training sessions conducted for staff to maintain awareness and compliance with security measures.
- **Audit and assessment reports:** Records from security audits, vulnerability assessments and penetration testing to evaluate system security and identify weaknesses.
- **Security controls implementation:** Evidence showcasing the deployment and effectiveness of security controls, such as access controls, encryption and authentication mechanisms.
- **Security governance reviews:** Documentation highlighting periodic reviews, updates or revisions made to security governance frameworks based on evaluations or changes in risk landscapes.

These evidence requirements validate a mobile money provider's commitment to robust security governance, ensuring adherence to policies, proactive risk management and a structured approach to addressing security-related concerns within their operations.

[30] ISO 9001:2015
[31] ISO/IEC 20000-1:2018
[32] ISO/IEC 27001:2005 Sec 4.2.1.d) and 5.1
[33] ISO 22301:2019
[34] ISO 31000:2009 Sec 4.3.3

Designing and developing secure systems, applications and networks[35,36,37,38]

Designing and developing secure systems, applications and networks, as per Principle 5 of the GSMA Mobile Money Certification, is crucial to thwart potential cyberthreats. This approach integrates robust security measures during the creation and implementation phases, ensuring resilience against vulnerabilities. Implementing encryption, access controls and stringent coding practices bolsters defences, safeguarding against unauthorised access or data breaches. Regular security testing and audits strengthen these measures, ensuring the integrity and confidentiality of user data and transactions.

By prioritising secure design and development, mobile money providers mitigate risks, instil user confidence and uphold the reliability and trustworthiness of their services in the face of evolving cyberthreats.

Under Principle 5 of the GSMA Mobile Money Certification, evidence requirements for designing and developing secure systems, applications and networks may include:

- **Secure design documents:** Records outlining the secure architecture, design specifications and risk assessments during the development phase.
- **Security standards adherence:** Evidence showcasing compliance with industry security standards and best practices during system/application development.
- **Secure coding practices:** Documentation highlighting the use of secure coding techniques and adherence to coding standards to mitigate vulnerabilities.
- **Security testing results:** Records from security testing, including vulnerability assessments, penetration tests and code reviews.
- **Access control mechanisms:** Evidence of robust access controls implemented within systems or applications to restrict unauthorised access.
- **Encryption implementation:** Documentation demonstrating the deployment of encryption protocols to protect sensitive data in transit and at rest.
- **Network security configurations:** Records indicating secure network configurations, firewalls, intrusion detection systems and other network security measures.
- **Patch management records:** Evidence showcasing procedures for timely security updates and patch management to address known vulnerabilities.
- **Security documentation and training:** Records indicating the provision of security documentation and training to development teams on secure development practices.
- **Security incident response plans:** Documentation outlining procedures for responding to security incidents and breaches during development and testing phases.

These evidence requirements validate the mobile money provider’s commitment to building secure systems, applications, and networks. They ensure adherence to secure design principles, implementation of robust security controls, and proactive measures to identify and mitigate security risks during the development lifecycle.

[35] ISO/IEC 20000–1:2018

[36] ISO/IEC 27001:2005 – 4.2.1. d) to g)

[37] ISO 22301:2012 Sec 6.1

[38] ISO 31000:2009 Sec 5

Security operations[39,40,41]

Robust security operations, integral to Principle 5 of the GSMA Mobile Money Certification, ensure swift detection and mitigation of security threats. They encompass proactive monitoring, incident response readiness and regular audits. Implementing security incident and event management systems aids in prompt threat identification, enabling immediate response and mitigation strategies. Intrusion detection systems and routine updates bolster defences against evolving risks. By prioritising these operations, mobile money providers can thwart security threats and ensure continuous service integrity, user data protection and adherence to stringent security protocols, fostering a secure and resilient mobile money ecosystem.

Under Principle 5 of the GSMA Mobile Money Certification, key evidence requirements for security operations are as follows:

- **Security policy and procedure documentation:** Evidence of established security policies, protocols and procedures within the organisation with periodic reviews, updates or revision notes.
- **Incident response documentation:** Records outlining incident response procedures and documentation of responses to security incidents encountered.
- **Security monitoring reports:** Evidence of continuous security monitoring activities, including logs, reports and analyses of security events and threats.
- **Security incident logs:** Records documenting security incidents, including their nature, impact and actions taken for resolution.
- **Security audits and assessments:** Reports from routine security audits, vulnerability assessments and penetration tests conducted to evaluate system security.
- **Security controls implementation records:** Documentation showcasing the implementation and effectiveness of security controls like access controls, encryption and intrusion detection systems.
- **Security patching records:** Evidence of procedures for timely application of security patches and updates to mitigate known vulnerabilities.
- **Employee training and awareness programmes:** Records demonstrating security training sessions and awareness programmes conducted for employees.
- **Security incident response testing:** Records of testing incident response plans through simulations or drills to ensure preparedness.

These evidence requirements substantiate the robustness of security operations within a mobile money provider's framework. They validate adherence to security protocols, proactive monitoring, incident response readiness, and overall vigilance against emerging threats within the mobile money ecosystem.

[39] ISO/IEC 20000-1:2018
[40] ISO 9001:2015
[41] ISO 31000:2009 Sec 4.5 and 5.6

Principle 6
Transparency

Mobile money providers should communicate the fees and terms and conditions to users in a transparent manner. This not only builds trust and loyalty in the service, but also helps users –often on low incomes – to manage their finances efficiently. This section highlights best practices that mobile money providers seeking to become certified should incorporate in their policies and implement.

Transparency of fees and terms and conditions

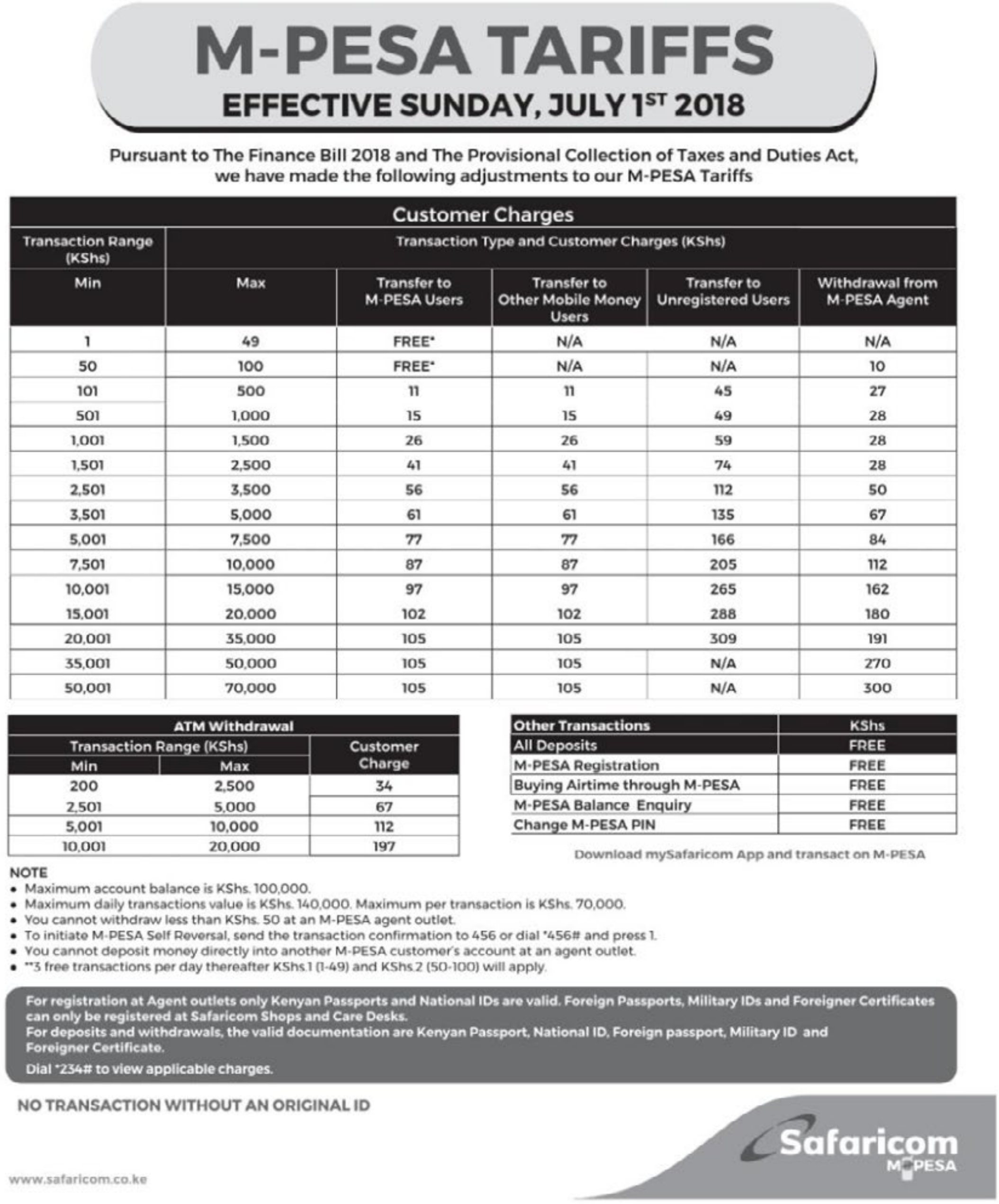
A mobile money provider should ensure they provide the fees and terms and conditions to customers in a transparent manner. Best practices in the industry require the provider to make the fee and key terms and conditions available to customers through all relevant channels, including the mobile money app menu, USSD menu, agent location and website. At the time of the transaction, the fee should also be made transparent to the customer on the platform or channel they use for the transaction and before they complete it, with an option to cancel the transaction if they do not agree with the fee.

Changes in fees should also be communicated to customers in advance. Safaricom's mobile money service, M-PESA, is an example of best practice in this regard. M-PESA has demonstrated transparency by communicating changes in fees and terms through an advertisement in the newspaper. However, it should be noted that there is no recommended lead time for making the changes public because this is a commercial matter and recommending one could lead to anti-competitive practices.

Mobile money providers should provide summaries of key terms and conditions in simple language, both at the beginning of the contract and through other means easily accessible to customers, such as SMS. These summaries should include the core information DFS consumers need, such as:

- All prices and fees, using definitions established by regulator
- The provider that is ultimately responsible for the service (e.g., if a bank is providing a service via a mobile money channel then the bank's role is clearly disclosed)
- Limitations, if any, on the consumer's ability to cash out
- Any explicit obligations of the customers (e.g., to maintain PIN secrecy)
- Under which circumstances the consumer bears the risk of loss and the provider is not liable (e.g., when fraud results from a consumer giving out their PIN)
- Where and how to complain if the consumer has a problem
- For digital credit products, relevant rates, as well as all delinquency and default penalties

The key terms and conditions should also be made clear to the customer before completing the transaction, and customers should have the option to cancel the transaction if they do not agree with the terms and conditions.



M-PESA TARIFFS

EFFECTIVE SUNDAY, JULY 1ST 2018

Pursuant to The Finance Bill 2018 and The Provisional Collection of Taxes and Duties Act, we have made the following adjustments to our M-PESA Tariffs

Customer Charges

Transaction Range (KShs)	Transaction Type and Customer Charges (KShs)				
Min	Max	Transfer to M-PESA Users	Transfer to Other Mobile Money Users	Transfer to Unregistered Users	Withdrawal from M-PESA Agent
1	49	FREE*	N/A	N/A	N/A
50	100	FREE*	N/A	N/A	10
101	500	11	11	45	27
501	1,000	15	15	49	28
1,001	1,500	26	26	59	28
1,501	2,500	41	41	74	28
2,501	3,500	56	56	112	50
3,501	5,000	61	61	135	67
5,001	7,500	77	77	166	84
7,501	10,000	87	87	205	112
10,001	15,000	97	97	265	162
15,001	20,000	102	102	288	180
20,001	35,000	105	105	309	191
35,001	50,000	105	105	N/A	270
50,001	70,000	105	105	N/A	300

ATM Withdrawal

Transaction Range (KShs)		Customer Charge
Min	Max	
200	2,500	34
2,501	5,000	67
5,001	10,000	112
10,001	20,000	197

Other Transactions	KShs
All Deposits	FREE
M-PESA Registration	FREE
Buying Airtime through M-PESA	FREE
M-PESA Balance Enquiry	FREE
Change M-PESA PIN	FREE

Download mySafaricom App and transact on M-PESA

NOTE

- Maximum account balance is KShs. 100,000.
- Maximum daily transactions value is KShs. 140,000. Maximum per transaction is KShs. 70,000.
- You cannot withdraw less than KShs. 50 at an M-PESA agent outlet.
- To initiate M-PESA Self Reversal, send the transaction confirmation to 456 or dial *456# and press 1.
- You cannot deposit money directly into another M-PESA customer's account at an agent outlet.
- **3 free transactions per day thereafter KShs.1 (1-49) and KShs.2 (50-100) will apply.

For registration at Agent outlets only Kenyan Passports and National IDs are valid. Foreign Passports, Military IDs and Foreigner Certificates can only be registered at Safaricom Shops and Care Desks.
For deposits and withdrawals, the valid documentation are Kenyan Passport, National ID, Foreign passport, Military ID and Foreigner Certificate.

Dial *234# to view applicable charges.

NO TRANSACTION WITHOUT AN ORIGINAL ID

Safaricom
M-PESA

www.safaricom.co.ke

Mobile money providers should make customer contracts available to consumers in readily and easily accessible ways, including in languages commonly spoken in the region and via multiple means, including both digital and print versions available at agent and customer care locations. Providers should also keep contracts as short and precise as feasible, and use simple wording that is easy for customers to understand.

Mobile money providers should also clarify in the terms and conditions the situations in which they are liable for outcomes that negatively affect customers, including, but not limited to: acts and omissions of agents, employees and third-party service providers (e.g., agent network managers), including cases of fraud; loss or harm due to network issues such as network downtime; and fraud related to DFS systems/platforms, including system or data breaches. They should also clarify that customers are liable in other cases.

Mobile money providers should review their terms and conditions regularly to ensure there are no unconscionable or unfair terms or practices, such as limiting access to recourse, misleading terms or omitting information about pricing or other key terms of service.

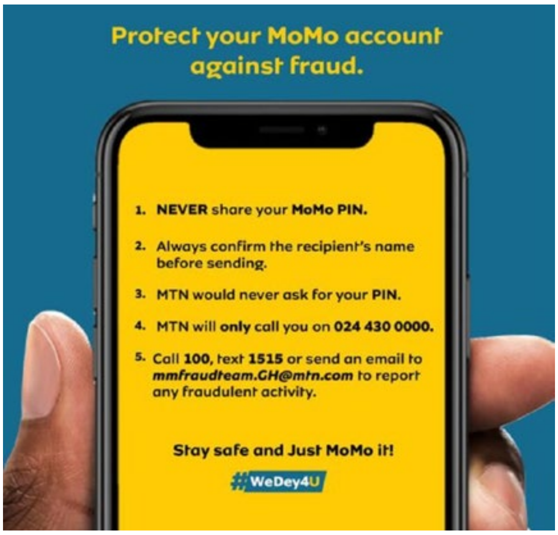
A provider should also ensure that they effectively communicate downtime to customers. Scheduled or planned downtimes should be communicated at least five days in advance. However, it is always difficult to give reasonable advance notice for emergency downtimes and there is no best practice. Based on the industry's record, the recommendation is to notify impacted customers of the downtime by SMS as soon as possible in advance.

Educating customers about safety and security

Mobile money providers should also educate their customers to use the mobile money service safely and securely. This is important because different customer segments have different levels of understanding of mobile money usage. Incorrectly entering an account number or sharing credentials with others leads to loss of funds and, eventually, erosion of trust in mobile money. Customer education should be carried out on a routine basis.

A few years ago, when not everyone had access to social media, mobile money providers used SMS and print media to raise awareness of how to use a mobile money account securely. Today, social media has become a channel for mobile money providers to create this awareness.

The following is an example of how MTN Ghana is using Facebook to generate customer awareness of safe mobile money use.



Protect your MoMo account against fraud.

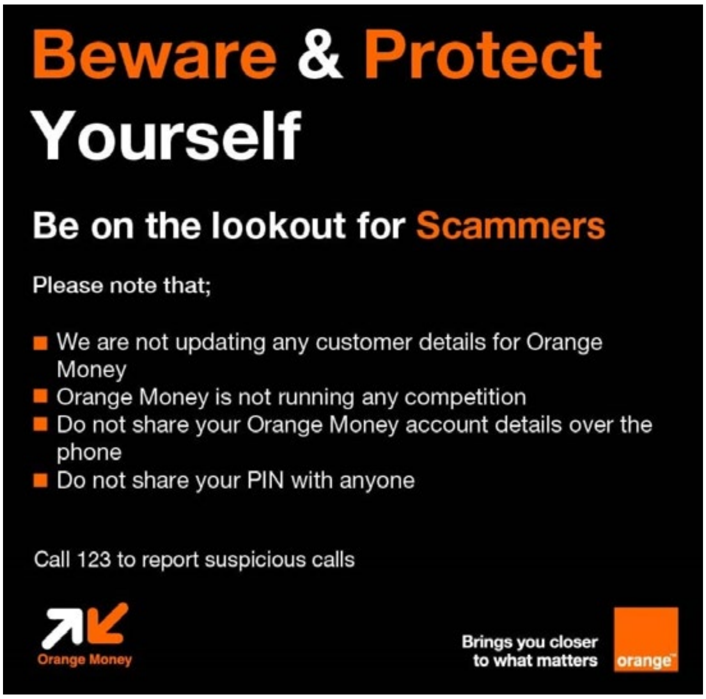
1. **NEVER** share your **MoMo PIN.**
2. Always confirm the recipient's name before sending.
3. **MTN** would never ask for your **PIN.**
4. MTN will **only** call you on **024 430 0000.**
5. Call **100**, text **1515** or send an email to ***mmfraudteam.GH@mtn.com*** to report any fraudulent activity.

Stay safe and Just MoMo it!

#WeDey4U

Source: Facebook

Similarly, Orange Money is using Facebook, among other channels, to generate customer awareness of using mobile money safely and keeping account details, including PINs, secure.[42] The following campaign was launched when scammers claiming to be Orange employees and affiliates tried to steal customer information and funds.



Beware & Protect Yourself

Be on the lookout for Scammers

Please note that;

- We are not updating any customer details for Orange Money
- Orange Money is not running any competition
- Do not share your Orange Money account details over the phone
- Do not share your PIN with anyone

Call 123 to report suspicious calls

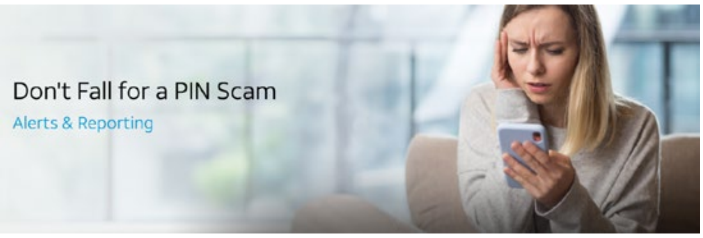
Orange Money
Brings you closer to what matters
orange

Source: Facebook

[42] Orange Botswana Facebook post, 29 September 2020.

Telenor Easypaisa is also using video campaigns to alert customers to the harmful effects of sharing their PIN and other credentials. It also advises customers to block such callers by calling the Easypaisa helpline.

Another example is the AT&T mobile campaign, "Don't Fall for a PIN Scam".[43]

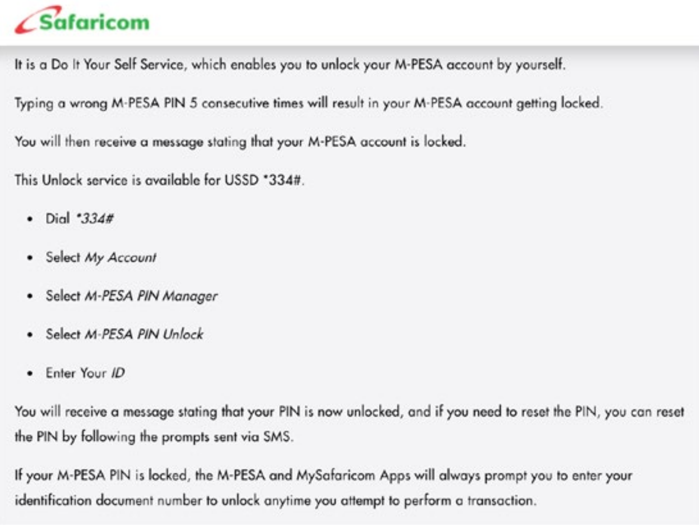


The following is an example of a hypothetical campaign. It is for illustrative purposes only and not based on an actual advertising campaign of a mobile money provider.

Campaign Title:
"Protect Your PIN, Secure Your Money"

Advertising copy: "Dear Valued Users, Your security matters to us! At [Mobile Money Provider], we're committed to ensuring the safety of your funds. Please remember, your PIN is your key to secure transactions. Never share your PIN with anyone, no matter the circumstance. It's your secret code to safeguard your hard-earned money. Protect it like your wallet. Together, let's keep your accounts safe and secure. For more tips on safeguarding your finances, visit our website or contact our support team."

While campaigns for keeping credentials safe are common, it is also important that mobile money providers explain to customers the impact of using incorrect credentials. A typical scenario in rural areas is customers who keep trying incorrect PINs when they have forgotten their PIN, not realising that this could lead to their account being blocked. Safaricom has demonstrated best practice by raising awareness of the consequences of entering an incorrect M-PESA account PIN repeatedly. They also take it a step further by explaining to customers the process for unlocking and setting a new PIN. All this can be done through a DIY process, yet another industry best practice.



It is a Do It Your Self Service, which enables you to unlock your M-PESA account by yourself.

Typing a wrong M-PESA PIN 5 consecutive times will result in your M-PESA account getting locked.

You will then receive a message stating that your M-PESA account is locked.

This Unlock service is available for USSD *334#.

- Dial **334#*
- Select *My Account*
- Select *M-PESA PIN Manager*
- Select *M-PESA PIN Unlock*
- Enter Your *ID*

You will receive a message stating that your PIN is now unlocked, and if you need to reset the PIN, you can reset the PIN by following the prompts sent via SMS.

If your M-PESA PIN is locked, the M-PESA and MySafaricom Apps will always prompt you to enter your identification document number to unlock anytime you attempt to perform a transaction.

Telenor Easypaisa has also enabled customers to change their PIN or unlock their Easypaisa account using a USSD account management menu[44]

[43] ATandT Cyber Aware web page: "Don't Fall for a PIN Scam".
[44] Easypaisa FAQs.

Principle 7
Customer service

Customer service is an important function of a mobile money service. Dealing with customers effectively and resolving their complaints is crucial to the success of the service. Otherwise, the mobile money provider is at higher risk of low brand ratings, as well as regulatory fines since some countries regulate certain aspects of customer service (number of complaints received and resolved in a timely manner, quality of service, incidents of fraud, etc.).

Key elements of a customer service policy

Developing a robust customer service policy is the first step in managing customer expectations and experience. Based on a review of the customer service manuals and policies of different mobile money providers, a strong corporate customer service policy should:

- **Detail** the mechanics of each product and service.
- **Ensure** customer orientation.
- **Offer** guidance on informing customers about relevant policies and procedures, including customer service channels, product terms, complaint mechanisms and transaction reversals.
- **Establish** a point of contact (POC) for each service. This is especially vital in joint service provisions, such as digital credit offered by a mobile money provider and a lending institution.
- **Reference** the transaction reversal policy.
- **Encompass** all available channels and platforms for customers to address comments and complaints.
- **Provide** a link to the customer service training manual for front-line staff and agents.
- **Guide** the process for complaints management and accessing external recourse mechanisms for customers.
- **Direct** customers to the platform that logs customer complaints and provide instructions on its use.
- **Define** SLAs for each process, such as complaints management and reversals.

Under Principle 7 of the GSMA Mobile Money Certification, evidence requirements for customer service policies might include:

- **Customer service policy documentation:** Records outlining the established customer service policies, procedures and protocols addressing user queries, complaints and dispute resolution.
- **Training records:** Evidence showcasing training sessions or materials provided to staff regarding customer service policies, ensuring uniformity and quality in service delivery.
- **Customer complaint logs:** Documentation of logs recording customer complaints, demonstrating the process and resolution mechanisms in place.
- **User feedback documentation:** Records or surveys capturing user feedback on customer service experiences, demonstrating the effectiveness of policies in addressing user needs.
- **Performance metrics:** Data or reports indicating key performance indicators (KPIs) related to customer service, such as response times, resolution rates and satisfaction levels.
- **Compliance records:** Evidence showcasing compliance with regulatory requirements concerning customer service policies and user protection.

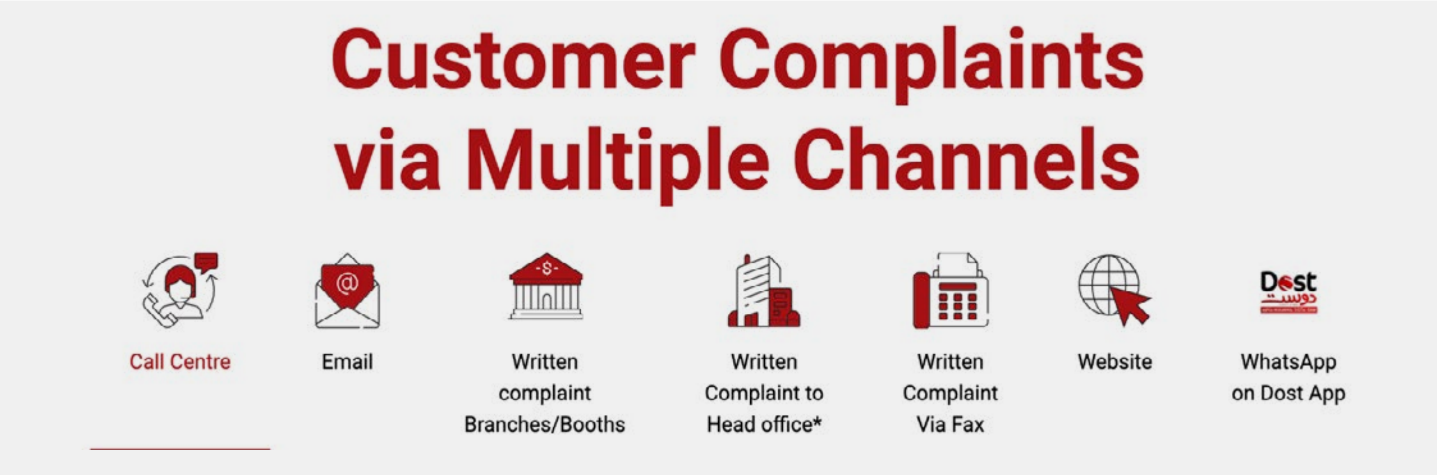
These evidence requirements validate a mobile money provider's commitment to establishing and adhering to robust customer service policies, ensuring prompt and effective resolution of user queries and complaints while enhancing user satisfaction within the mobile money ecosystem.

Complaints management process

At the heart of a first-class mobile money service is the user. Therefore, listening to customer complaints and resolving them effectively should be the top priority of a mobile money provider. An effective complaints management process includes the following:

- Providing a complaints channel to the customer
- Creating awareness of the process
- Recording the complaint
- Verifying the customer’s identity
- Acknowledging the complaint and providing a resolution timeline
- Providing resolution along with the option for external recourse if the customer is not satisfied with the outcome

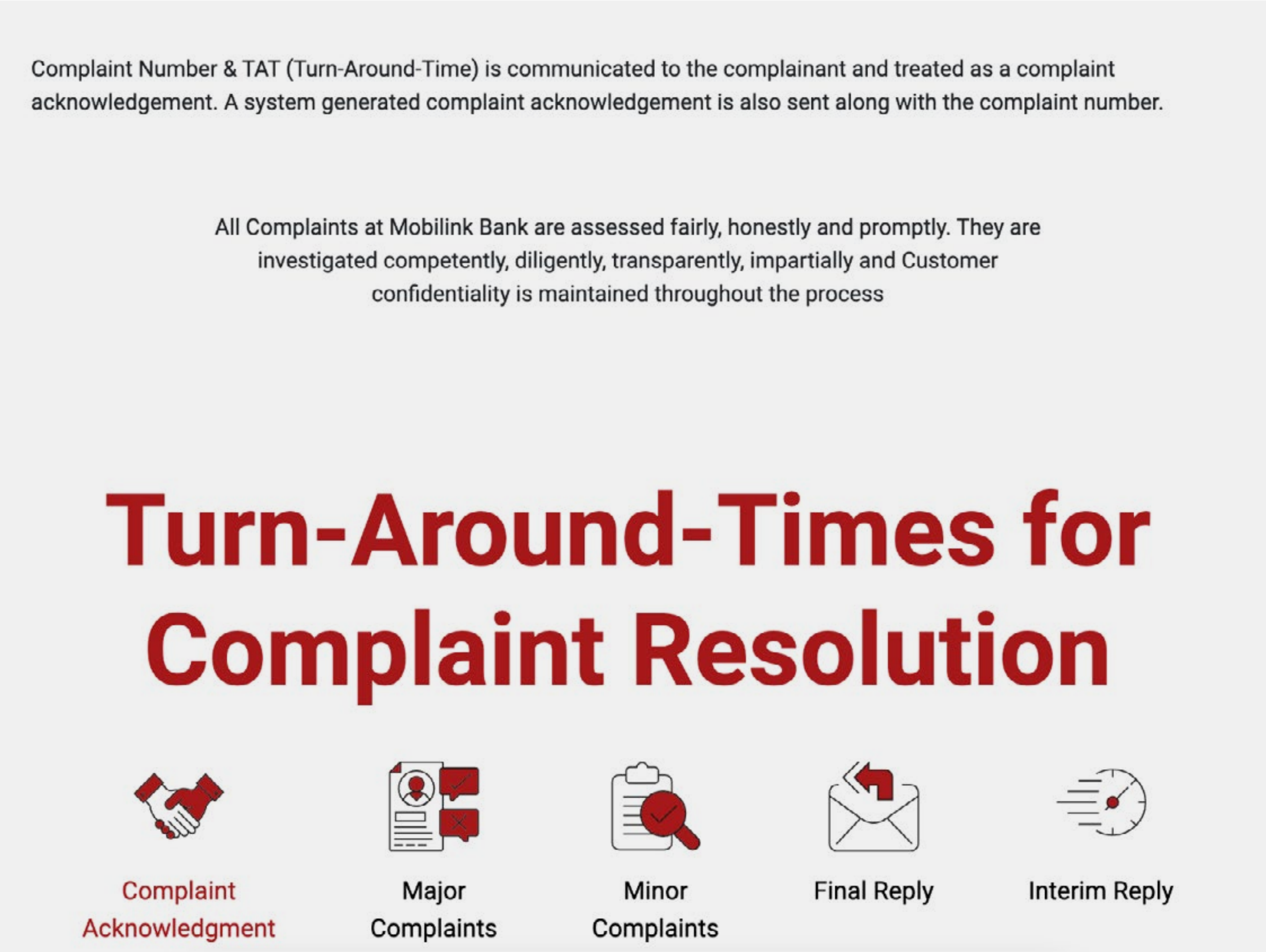
As a best practice example, Mobilink Bank, which works with JazzCash, provides a transparent complaints management process[45] and a variety of channels for customers to voice their complaints, allowing them to select their preferred method.


Customer Complaints via Multiple Channels
Call Centre
Email
Written complaint Branches/Booths
Written Complaint to Head office*
Written Complaint Via Fax
Website
Dost
WhatsApp on Dost App

[45] Mobilink Bank “Complaint Logging Process” web page.

Mobilink Bank also demonstrates transparency in their complaints resolution timelines, setting clear expectations for customers.

If customers are dissatisfied with the outcome of the complaints resolution, they can pursue external recourse with the financial sector regulator (State Bank of Pakistan).

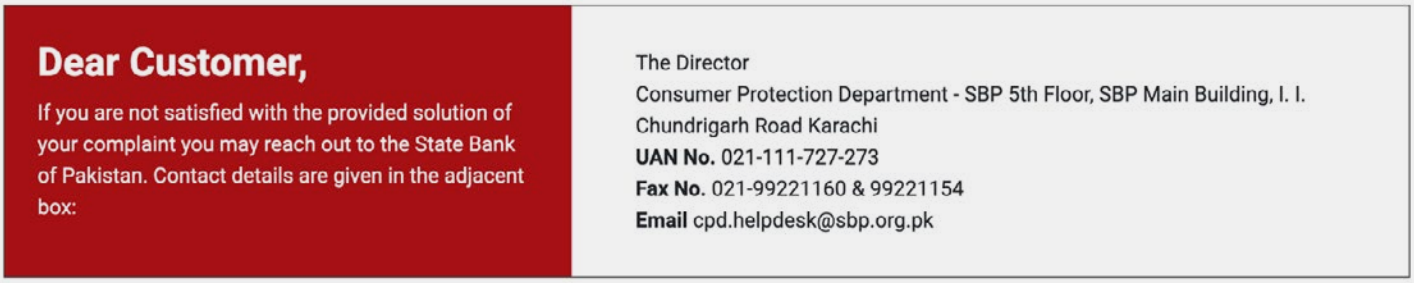


Complaint Number & TAT (Turn-Around-Time) is communicated to the complainant and treated as a complaint acknowledgement. A system generated complaint acknowledgement is also sent along with the complaint number.

All Complaints at Mobilink Bank are assessed fairly, honestly and promptly. They are investigated competently, diligently, transparently, impartially and Customer confidentiality is maintained throughout the process

Turn-Around-Times for Complaint Resolution

Complaint Acknowledgment	Major Complaints	Minor Complaints	Final Reply	Interim Reply
Within **48 hours** of receipt of complaint.	Require more than **7 working days** for resolution.	May be resolved within **7 working days**.	Within **7 working days** for minor complaints. Within **30 days** for fraud related complaints.	After **10 working days**. Resolution within **15 days**.



Dear Customer,

If you are not satisfied with the provided solution of your complaint you may reach out to the State Bank of Pakistan. Contact details are given in the adjacent box:

The Director
Consumer Protection Department - SBP 5th Floor, SBP Main Building, I. I. Chundrigarh Road Karachi
UAN No. 021-111-727-273
Fax No. 021-99221160 & 99221154
Email cpd.helpdesk@sbp.org.pk

Transaction reversals

There were 65 billion mobile money transactions with an accumulated value of USD 1.26 trillion in 2022.[46] Given the scale of transactions and the number that could go into the wrong account, the GSMA Mobile Money Certification has a strong focus on transaction reversal mechanisms.

A mobile money provider should develop a stand-alone policy for transaction reversals that should be embedded in the corporate customer service policy. Based on a review of the respective policies of mobile money providers, a best practice for transaction reversal should include the following elements:

- The policy should include a clear procedure for reversals, including off-net reversals and fraudulent reversals.
- Circumstances that do not permit reversals, for example, fraudulent retail reversals attempted when goods have been purchased or in situations where money has already been cashed out by the recipient.
- The process for self-initiated reversals (SIR) should also be clearly stated, including reference to the terms and conditions. SIR is a mobile money transaction reversal whereby a customer can initiate a transaction reversal to hold an amount wrongly sent to another customer (P2P), or where a customer enters an incorrect TILL number during a withdrawal at an agent point and initiates a reversal to hold the specific amount. Although very few mobile money providers are allowing self-initiated reversals, these can help save human resource costs, reduce call centre traffic and increase efficiencies. In the following box, Vodafone[47] explains how their self-initiated reversals work.
- Clear time limits should be stipulated with each type of reversal.

- A self-reversal can be done by dialling *110#, go to 7 My Account, 7 Self-Service and select 2 for Self-Reversal.
- To reverse a transaction, you can select from your last 5 transactions made. Alternatively, you can enter transaction IDs without the preceding zeroes.
- A reversal can be initiated on a VCASH voucher transaction and on a TILL number, but not on an online transaction (utilities, betting, etc.)
- The VCASH back-office team will investigate the self-initiation request and solve the issue within 24 hours so that the money can be reversed in the account.
- There is a daily limit of three transactions that may be reversed and a transaction which is more than 7 days old cannot be reversed.
- Self-initiation request for a reversal has two key benefits. (1) A recipient cannot withdraw an amount on a transaction wrongly sent to them. (2) It is faster as customers do not need to call our contact centre after a wrong transaction is made.
- The self-initiation does not freeze the account of the wrong recipient. It rather holds the specific transaction or amount on which a reversal is being made.
- Self-initiated reversal requests do not incur a charge.

[46] GSMA. (2023). *State of the Industry Report on Mobile Money 2023*.

[47] Vodafone “Self-Initiated Reversals (SIR) FAQs” web page.

Principle 8
Data privacy

Data privacy has become increasingly important and embedded in the lives of everyone using technology. Users share their personal data with service providers, which puts greater responsibility on the providers to protect the data they collect. Despite the implementation of data privacy processes, over the past decade, phenomenal values of regulatory fines have been linked to data privacy violations globally.

Objective of a data privacy programme

The risks of data privacy violations are high in the mobile money industry because loss of data could also involve loss of personal funds stored in a mobile money account. Since fraudsters gain access to personal data, they can use this to gain access to mobile money funds or even funds stored in accounts held by other financial services providers (FSPs), such as banks and fintechs. Therefore, having a strong and robust data privacy policy is now a necessity for any mobile money provider regardless of where it operates.[48]

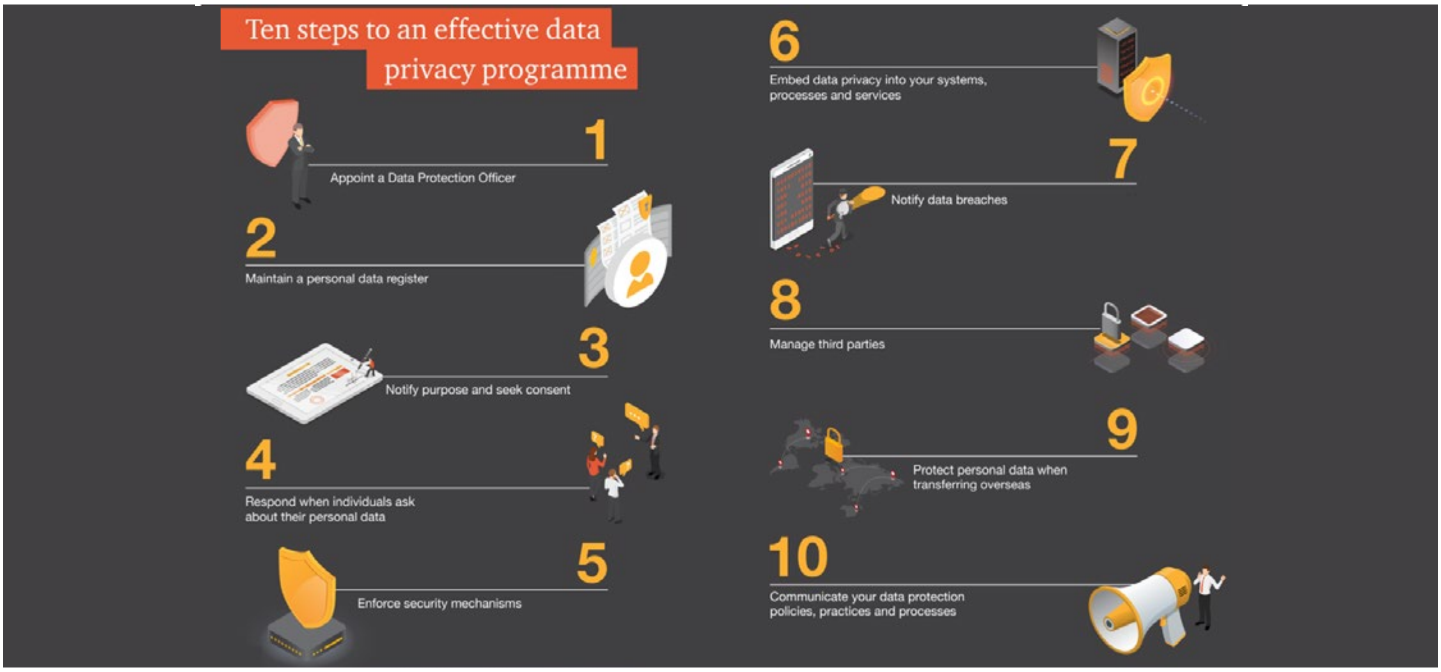
[48] Mobile money services are now available in more than 100 countries. See: www.gsma.com/sotir

PwC's data privacy framework

The world of data privacy can be quite complicated and is constantly changing. This can pose many difficulties for mobile money providers as they navigate the uncertainty of how to handle personal data. The implementation of the General Data Protection Regulation (GDPR) and ongoing efforts to create local data privacy laws are making it challenging for businesses to keep up with the evolving regulatory landscape and adjust their practices accordingly.

To streamline the process and assist organisations with their data privacy compliance efforts, PwC has compiled the *Data Privacy Handbook*. This comprehensive toolkit caters to organisations processing personal data, offering a practical path for compliance and valuable resources and guidance to evaluate current business practices and implement necessary improvements in line with best practices in data privacy.

The toolkit provides 10 steps that can be used as a template for developing an effective data privacy programme. Starting with the appointment of a Data Protection Officer, it emphasises maintaining a comprehensive data register, obtaining consent transparently and addressing personal data inquiries promptly. It suggests that rigorous security enforcement, systematic integration of privacy measures and effective breach notifications are vital. Managing third-party relationships and safeguarding data during international transfers are highlighted. The document underscores the importance of clear communication on data protection policies to fostering trust and transparency within the organisation and with stakeholders.


Ten steps to an effective data privacy programme
1
Appoint a Data Protection Officer
2
Maintain a personal data register
3
Notify purpose and seek consent
4
Respond when individuals ask about their personal data
5
Enforce security mechanisms
6
Embed data privacy into your systems, processes and services
7
Notify data breaches
8
Manage third parties
9
Protect personal data when transferring overseas
10
Communicate your data protection policies, practices and processes

The European Union's GDPR

The European Union (EU) GDPR[49] is an excellent example of, and ambitious reference for, a robust and strong data privacy programme. It consists of seven protection and accountability principles:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

Even though it was developed for the EU, it has profoundly influenced the data privacy practices and policies in many countries outside the EU. In some cases, mobile money providers that are headquartered in the EU but also operate in countries outside the Union, find it cost-effective and operationally efficient to have GDPR-based data privacy policies[50] as a standard across their footprint. Since large mobile money providers also partner with tech giants and other large digital operators, implementing data privacy policies that are based on a common legal framework accepted[51] globally is recommended.

[49] EU General Data Protection Regulation (GDPR): https://gdpr-info.eu/
[50] Interviews with telecom operators that offer services both in the EU and outside.
[51] Although not required across the globe.

Data Protection Officer: job description and responsibilities

Every organisation must appoint a Data Protection Officer (DPO) to monitor internal compliance with applicable data protection laws, advise on data protection obligations and act as a point of contact for individuals and data protection authorities. It is recommended that large mobile money providers have a dedicated DPO whereas smaller providers may assign the role to an individual in a compliance department unless it is against the law in the country.

Job description

Title: Data Protection Officer

Role: Oversee and manage data protection and privacy measures within the organisation

Reports to: Senior management or board of directors

Location: On-site

Responsibilities

Compliance oversight: Ensure compliance with data protection laws, regulations and internal policies

Policy development: Develop and implement data protection policies and procedures

Educating staff: Educate employees on data protection laws, policies and best practices

Data mapping and audits: Conduct data mapping, audit and risk assessments to identify vulnerabilities

Handling requests: Manage and respond to data subject requests and inquiries

Security measures: Implement and monitor security measures to safeguard data

Breach management: Develop incident response plans and manage data breach incidents

Vendor management: Oversee and manage relationships with third-party vendors handling data

Training and awareness: Organise training sessions and awareness programmes on data protection

Reporting: Prepare and submit reports to senior management or regulatory authorities as required

The DPO serves as a focal point for data protection matters, ensuring the organisation adheres to privacy laws, mitigates risks and fosters a culture of data protection and compliance across all levels of the organisation.

Important aspects of a data privacy policy implemented by international mobile money providers with strong and robust practices also include the following. Note that these are in line with the GDPR principles and go beyond what is typically required by financial regulators in mobile money markets. Therefore, these collectively form international best practices that can help mobile money providers demonstrate compliance with the GSMA Mobile Money Certification.

- Consent is required for collection, processing and storage of personal data.
- Collect personal data for a specific and legitimate purpose. It should be adequate and relevant to the purpose and not exceed what is required.
- Explicitly state what data is being collected, processed or stored. This may include the customer's identity and SIM-card registration information, including name, photograph (including through CCTV), address, location, phone number, ID type and number, date of birth, email address, age, gender and mobile number portability records, along with other personally identifiable information.
- Explicitly state how and when information is collected and subsequently processed or stored. This may include when registering an account, buying a service or product, interacting with agents, performing reference checks with third parties, calling or visiting customer services and requesting parking at a provider's location, among others.
- Explicitly state how the data is used or processed. This may include verifying the customer's identity, conducting reference checks, providing the service, responding to queries, complying with legal and regulatory requirements, preventing financial crime and fraud and for research to improve the service, among others.
- Process the data in a lawful, fair and transparent manner.
- Data collected and retained should be accurate and kept up to date (where necessary). Inaccurate data must be rectified or erased without delay.
- The data must be collected, processed and stored securely.
- The data must be kept in a form that permits identification with the data subject for no longer than necessary.
- Explicitly state how the data is handled when transferred outside the jurisdiction (where legally permitted).

Rights of data subjects

The rights of the data subject must be explicitly stated in the policy. The following are crucial and should be included. It is recommended that these rights are stated in simple language, in accordance with the country's laws, so that those with low literacy levels can also understand their fundamental rights with respect to data privacy.

- Right of access to personal information of the data subject, held by the provider
- Rights to rectification and erasure of personal data
- Right not to be subjected to automated decision-making (on key decisions such as credit applications or for profiling)
- Right to object (e.g., data monetisation or marketing purposes)

Operational aspects

It is also recommended that mobile money providers enforce similar policies at the agent and business partner level, so that the harmful effects of a breach at a related third party are managed effectively.

The policy must be dated and should be signed (when it is stored or communicated offline). It should be revised as soon as changes in the business environment merit an update to the policy.

Contact details should be provided to report incidents and to request information or manage data. Ideally, a phone number, email address, web form and postal address should be included.

Data breach

Reporting data breaches is crucial under Principle 8 of the GSMA Mobile Money Certification. It ensures swift response and mitigation, minimising potential harm to users and the integrity of the mobile money ecosystem. Timely reporting facilitates regulatory compliance, builds trust with users and allows for corrective measures to prevent future incidents. It also aligns with transparency principles, enabling authorities to assess the severity of breaches and enforce necessary actions. Proactive and transparent reporting not only safeguards user data, but also maintains the credibility and reliability of the mobile money service in the face of evolving cybersecurity threats.

Under Principle 8 of the GSMA Mobile Money Certification, key evidence requirements for data breaches might include:

- Breach incident reports: Documentation detailing incidents of data breaches, including the nature, scope and impact on users and the system.
- Breach response procedures: Records outlining the steps taken in response to data breaches, including containment, recovery and notification processes.
- Notification records: Evidence showcasing notifications sent to affected users or relevant authorities following a data breach incident.
- Post-breach analysis: Reports or documentation detailing the analysis and lessons learned from data breach incidents, along with improvements made to prevent recurrence.
- Documentation of remediation: Records demonstrating actions taken to mitigate the effects of the breach and strengthen security measures.
- Regulatory compliance records: Evidence showcasing compliance with regulatory requirements regarding data breach reporting and management.

These evidence requirements validate a mobile money provider’s proactive approach to handling data breaches. They ensure the provider has robust processes in place for detecting, responding to and mitigating data breaches, thereby safeguarding user data and upholding the integrity of the mobile money service.

Annexes

Annex 1
Methodology

We reviewed the criteria in the GSMA Mobile Money Certification Excel toolkit to understand the overlap between indicators and the evidence requirements.

Since policies and processes varied widely among mobile money providers due to the regulatory frameworks in place, size of the provider, scope of products offered and level of risks, the guidance presents the minimum that should be explicitly stated in a policy document for each sub-principle or group of indicators.

This guidance supplements the content of the Mobile Money Certification Assessment Toolkit and should be read in conjunction with it.

Considering the dynamic nature of the digital finance industry, mobile money providers will continue to update their policies and procedures. It is recommended that this guidance is also reviewed for updates by the GSMA in line with industry developments.

Annex 2 Recommended reading

The following list is for mobile money providers interested in understanding the policy guidelines of international institutions and other organisations. It is for reference only.

#	P	Guideline
	P1	https://www.handbook.fca.org.uk/handbook/CASS/7/13.html
	P1	https://www.legislation.gov.uk/uksi/2017/752/contents/made
	P1	https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf
	P1	https://www.iso.org/standard/73906.html
	P2	International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (The FATF Recommendations)
	P2	MLRO (Financial Conduct Authority Handbook)
	P2	KYC Innovations, Financial Inclusion & Integrity (Alliance for Financial Inclusion)
	P2	Orange Botswana KYC Form
	P3	https://www.iso.org/standard/70636.html
	P4	https://www.iso.org/obp/ui/en/#iso:std:iso-iec:20000:-1:ed-3:v1:en
	P4	https://www.iso.org/standard/72120.html
	P4	https://www.iso.org/standard/75652.html
	P4	https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en
	P4	https://www.iso.org/standard/75107.html
	P4	https://www.iso.org/standard/75106.html
	P5	https://www.iso.org/standard/62085.html
	P5	https://www.iso.org/standard/70636.html
	P5	https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en
	P5	https://www.iso.org/news/2012/06/Ref1602.html
	P5	https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en
	P6	MTN SLAs
	P6	Mobilink Bank Customer Awareness Material
	P7	Mobilink Bank Complaint Management Process
	P7	Vodafone Reversals
	P8	Data Privacy Handbook (PWC)
	P8	Data Protection and Privacy Laws (World Bank, ID4D)
	P8	General Data Protection Regulation
	P8	The New Rules of Data Privacy (Harvard Business Review, 2022)

Annex 3
Waiver of Liability

The Guidance recognises that mobile money market dynamics vary from one region to another and there are differences between regulatory frameworks. Therefore, this document aims to provide guidance for a broad framework based on excerpts from high-level policies and procedures that providers may wish to consider when demonstrating compliance with the GSMA Mobile Money Certification principles with the understanding that this guidance does not override the purview of national regulatory authorities. Therefore, this guidance document serves as a guide only without giving rise to any liability for the GSMA, GSMA Mobile Money Certification Body, Assessors, Consultants or any related parties whatsoever.

GSMA Head Office
1 Angel Lane
London EC4R 3AB
United Kingdom

Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601