Defining and promoting excellence in the provision of mobile money services

Contents

Introduction

The GSMA Mobile Money Certification

The GSMA Mobile Money Certification is a global initiative to bring safe, transparent and resilient financial services to millions of mobile money users around the world.

Over the past decade, mobile money has evolved from a niche product in a small number of markets to an emerging market phenomenon, bringing reliable financial services to previously unbanked populations. Mobile money has evolved into the leading payment platform for the digital economy in many emerging markets. With 866 million registered accounts as of December 2018, the industry is now processing over $1.3 billion dollars a day.

A key ingredient in the success of mobile money has been trust. The Certification will help to take the industry to the next level by improving quality of services and customer satisfaction, facilitating the implementation of trusted partnerships, building trust with regulators and encouraging the implementation of appropriate and proportional regulatory standards.

Background

The GSMA Mobile Money Certification is the result of years of collaboration between the GSMA and the mobile money industry, to increase trust and transparency in the provision of mobile money services. Beginning with the launch of the GSMA Code of Conduct in late 2014, the GSMA worked together with providers in Africa, Latin America, and Asia to understand the challenges of their business and the best practices in these markets.

To develop the certification criteria, the GSMA led a three-year consultative process involving mobile money providers and independent expert consultants. The criteria were developed and tested through the self-assessments of 39 mobile money providers. In 2017 the GSMA contracted Alliances Management, an independent certification management company, to manage the scheme.

The benefits of becoming Certified

Certified organisations are at the forefront of the mobile money industry. They have proven that they are serious about protecting the rights of consumers, delivering reliable and secure services, and combatting money laundering and the financing of terrorism. Their business practices are amongst the very best in the industry.

Fundamentally, the Certification is about enhancing trust and empowering consumers to make more informed choices about their financial services. This encourages mobile money adoption and advances financial inclusion. It gives assurances to potential financial partners that robust controls are in place, facilitating interoperability and encouraging integration into the financial ecosystem. The potential to collaborate, innovate and integrate with business partners will also be enhanced.

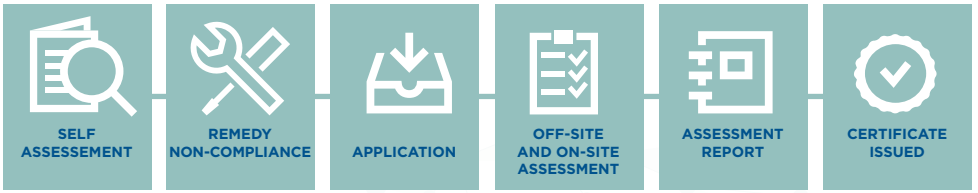
By defining industry best practice, the Certification aims to build trust with regulators and encourage the implementation of appropriate and proportional regulatory standards. Enhancing trust in mobile money is in the collective interest of the private sector, governments, regulators, and consumers. Society as a whole stands to gain from the digitisation of financial services.

The Principles of the Certification

The Certification comprises eight principles, which are further divided into sub-principles. These principles are explained in detail in the body of this document. The eight principles are:

1. **Safeguarding of Funds:**	Safeguard customer funds against the risk of loss
2. **AML/CFT/Fraud:**	Combat money laundering, terrorist financing and fraud
3. **People Management:**	Manage staff, agents, and third parties correctly
4. **Quality of Operations:**	Operate the service well and reliably
5. **Security of Systems:**	Ensure the security of the systems supporting the service
6. **Transparency:**	Communicate fees, T&Cs and information transparently to customer
7. **Customer Service:**	Effectively address customer service requests and complaints
8. **Data Privacy:**	Protect customers' personal data

The Certification process



For more information about the GSMA Mobile Money Certification, including details of the certification process, visit **gsmamobilemoneycertification.com** or email **mm@gsmamobilemoneycert.com.**

Principle 1: Safeguarding of Funds

Safeguard customer funds against the risk of loss

1.1 Protection against loss due to the failure of the bank, provider, or another party

Providers shall take measures to ensure that funds are protected in the case of insolvency of provider, custodial bank, or other entity

1.1.1 Providers shall ensure that funds equal to the total value of outstanding mobile money liabilities are held in one or more custodial accounts on behalf of the mobile money users

1.1.2 Providers shall ensure that user funds are ring-fenced to prevent attachment from the creditors of the provider in the event of a provider's insolvency

1.1.3 Providers shall take measures to mitigate the risk of loss of funds due to insolvency of the bank, bond issuer, or other entity in which funds are invested

1.2 Protection against settlement risk

Providers shall take measures to ensure that funds are not at risk due to the process of settlement with banks and other financial partners

1.2.1 Where feasible, providers shall only authorise customer transactions in which the debiting and crediting of mobile money accounts is processed in real time

1.22 Providers shall regularly reconcile transactions and settle balances with financial ecosystem partners*

* For the purposes of the Mobile Money Certification, "financial ecosystem partners" are entities that are connected to the mobile money service in order to provide a financial service. Examples include, but are not limited to, banks (custodial banks and other account-holding banks), entities that send or receive bulk payments, aggregators, merchants using Point of Sale devices, ATM providers, and other payment service providers (national and international).

Principle 2: AML/CFT/Fraud Prevention

Combat money laundering, terrorist financing and fraud

2.1 Effective AML/CFT policies and procedures
Providers shall develop effective policies and procedures for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) compliance

2.2 Senior management commitment to AML/CFT
Senior management shall demonstrate their commitment to AML/CFT compliance through proper oversight

2.3 Appointed AML/CFT manager (money-laundering reporting officer)
Providers shall appoint a qualified money-laundering reporting officer (MLRO) to promote and monitor compliance with AML/CFT-related obligations

2.4 Software to monitor transactions
Providers shall create a system to monitor transactions for AML/CFT and anti-fraud purposes

2.5 Risk-based KYC requirements and transaction/balance limits
Providers shall collect KYC and screen customers, and apply risk-based limits or blocks on transactions and account balances

2.5.1 Providers shall adequately identify clients

2.5.2 Providers shall place appropriate risk-based transaction and balance limits on accounts, depending upon the strength of customer identification and verification

2.5.3 Providers shall have the ability to block account transactions under certain circumstances.

2.5.4 Providers shall screen accounts using domestic and international money laundering, terrorist financing, and sanctions watch lists

2.6 Staff and agent AML/CFT training procedures
Providers shall train staff and agents in AML/CFT procedures, monitor their compliance and take action against violations

2.6.1 Providers shall ensure that staff and agents are properly trained in AML/CFT procedures.

2.6.2 Providers shall monitor staff and agent compliance with AML/CFT procedures

2.7 Fraud management
Providers shall develop risk-based policies and measures for fraud detection and prevention

Principle 3: People Management

Manage staff, agents, and third parties correctly

3.1 Due diligence policies and procedures
Providers shall conduct proper due diligence on potential staff, agents and entities providing outsourced services

3.2 Training of staff and agents
Providers shall develop and implement training programmes for staff and agents

3.2.1 Providers shall develop and implement training programmes for staff

3.2.2 Providers shall develop and implement training programmes for agents

3.3 Contractual agreements
Providers shall establish written agreements governing their relationship with agents and entities providing outsourced services

3.3.1 Providers shall establish written agreements governing their relationship with agents and entities providing outsourced services

3.3.2 Providers shall assume responsibility for actions taken on their behalf by their agents (and any sub-agents) under the provider-agent contract

3.4 Management of staff, agents and entities providing outsourced services
Providers shall develop policies and processes for ongoing management and oversight of staff, agents and entities providing outsourced services

Principle 4: Quality of Operations

Operate the service well and reliably

4.1 Board and senior management oversight of the mobile money service
Providers shall ensure that the Board of Directors and senior management establish effective management oversight

4.2 Service-level management and reporting
Providers shall manage technical and business operations according to service levels

4.2.1 Providers and partners should operate technical systems properly and manage service levels

4.2.2 Providers and partners should manage business operations and service levels

4.3 Capacity management
Providers shall take steps to ensure sufficient service capacity through forecasting, monitoring, and testing

4.4 Incident and problem management
Providers shall set up an incident management process to restore the service within agreed service levels and to investigate root causes of problems

4.5 Change and configuration management
Providers shall develop processes to ensure that systems and applications remain robust and secure following system and configuration changes

4.6 Enterprise risk management
Providers shall establish a risk management framework for identifying, assessing, and controlling risks

4.7 Business continuity
Providers shall develop effective business continuity and contingency plans

Principle 5: Security of Systems

Ensure the security of the systems supporting the service

5.1 Security governance

Providers shall implement governance mechanisms to ensure that security policies are defined and implemented with ongoing management

- 5.1.1 Providers shall develop, implement, and regularly review a formal security policy for mobile money services
- 5.1.2 Providers shall train staff about their security responsibilities
- 5.1.3 Providers shall ensure policies are in place for the secure handling of information and assets
- 5.1.4 Providers shall ensure the protection of their assets that are accessible by suppliers and third parties

5.2 Designing and developing secure systems, applications and network

Providers shall ensure that the systems, applications and network that support mobile money are designed and developed securely

- 5.2.1 Providers shall ensure that data is protected by cryptography and network security controls
- 5.2.2 Providers shall ensure that systems and applications are designed and developed securely and are thoroughly tested

5.3 Security operations

Providers shall implement processes to manage all systems and operations securely

- 5.3.1 Providers shall Identify, assess and monitor security risks
- 5.3.2 Providers shall properly identify and authenticate system users
- 5.3.3 Providers shall limit access to customer data on a “need to know” basis
- 5.3.4 Providers shall limit physical access to systems
- 5.3.5 Providers shall ensure correct and secure operations of information processing
- 5.3.6 Providers shall develop processes to ensure that all transactions and user activities are logged with appropriate audit trails
- 5.3.7 Providers shall regularly test security systems and processes
- 5.3.8 Providers shall ensure continuity of information security
- 5.3.9 Providers shall develop a process to identify, address, and monitor security incidents and security-related complaints

Principle 6: Transparency

Communicate fees, T&Cs and information transparently to customers

6.1 Effective disclosure and transparency
Providers shall ensure that users are provided with clear, prominent, and timely information regarding fees and terms and conditions

6.2 Education of customers about safety and security
Providers shall educate customers about how to use mobile money services safely and securely

Principle 7: Customer Service

Effectively address customer service requests and complaints

7.1 Customer service policies and procedures
Providers shall develop and publish customer service policies and procedures

- 7.1.1 Providers shall develop customer service policies and procedures
- 7.1.2 Providers shall inform customers of customer service policies and procedures
- 7.1.3 Providers shall develop specific policies for handling reversals

7.2 Availability of customer service support
Providers shall provide an appropriate mechanism to address customers' questions and problems

7.3 External recourse mechanisms
Providers shall specify how disputes can be resolved if internal resolution fails

Principle 8: Data Privacy

Protect customers' personal data

8.1 Governance of data privacy
Providers shall comply with good practices and relevant regulations governing customer data privacy

8.2 Data privacy transparency
Providers shall ensure that users are provided with clear, prominent, and timely information regarding their data privacy practices

8.3 Customers' control of their personal data
Providers shall ensure that customers are informed of their rights and have opportunities to exercise meaningful choice and control over their personal information

8.4 Minimisation of personal data collection and retention
Providers shall limit the personal information that is collected from customers and is retained, used, or shared

Annex: Definition of mobile money

Mobile money is a transformational service that uses information and communication technologies to extend the delivery of financial services to clients who cannot be reached with traditional branch-based financial services.

A service is considered to be mobile money if it meets the following criteria:
In 2018, we revised our definition of mobile money. Now, a service is considered a mobile money service if it meets the following criteria:

1. A mobile money service includes transferring money and making and receiving payments using the mobile phone.
2. The service must be available to the unbanked, e.g. people who do not have access to a formal account at a financial institution.
3. The service must offer a network of physical transactional points which can include agents, outside of bank branches and ATMs, that make the service widely accessible to everyone.
4. Mobile banking or payment services (such as Apple Pay and Google Wallet) that offer the mobile phone as just another channel to access a traditional banking product are not included.
5. Payment services linked to a traditional banking product or credit card, such as Apple Pay and Google Wallet, are not included.

For more information about the GSMA Mobile Money Certification, including details of the certification process, visit **gsmamobilemoneycertification.com** or email **mm@gsmamobilemoneycert.com.**






GSMA
MOBILE MONEY
CERTIFICATION