Code of Conduct for Mobile Money Providers

VERSION 2 - OCTOBER 2015

Introduction

This Code of Conduct identifies principles aimed at promoting mobile money[1] providers' adoption of consistent risk mitigation practices in certain critical areas of their business.

For the mobile money sector to continue to drive the growth of the digital finance ecosystem, mobile money providers ("providers") have adopted a Code of Conduct aimed at ensuring that their services are sound, the channel is secure, and the customer is treated fairly. The Code of Conduct will support the continued growth of the industry by:

- Improving quality of services and customer satisfaction;
- Facilitating the implementation of trusted partnerships; and
- Building trust with regulators and encouraging the implementation of appropriate and proportional regulatory standards.

The providers who subscribe to the Code formalise their commitment to eight principles underpinning three key areas of importance:

i. soundness of services;
ii. security of the mobile network and channel; and
iii. fair treatment of customers.

By endorsing the Code, providers commit to:[2]

1. Safeguard customer funds against risk of loss;
2. Maintain effective mechanisms to combat money laundering and terrorist financing;
3. Equip and monitor staff, agents, and entities providing outsourced services to ensure that they offer safe and reliable services;
4. Ensure reliable service provision with sufficient network and system capacity;
5. Take robust steps to ensure the security of the mobile network and channel;
6. Communicate clear, sufficient and timely information to empower customers to make informed decisions;
7. Develop mechanisms to ensure that complaints are effectively addressed and problems are resolved in a timely manner; and
8. Follow good data privacy practices when collecting, processing, and/or transmitting customers' personal data.

A NOTE ABOUT AMENDMENTS TO VERSION 2

The following amendments have been made in order to streamline the Code and ensure full coverage of all relevant topics:

- **Sub-principles within Principles 1, 3, 4 and 5 have been amended.**
- **Principle 8 has been reworded to clarify that it addresses data privacy, not data security. The sub-principles remain unchanged.**
- **Principles 2, 6 and 7 remain unchanged.**

1. See Annex for a definition of mobile money for the purposes of this document.
2. In many countries, local laws and regulations address some or all of the topics identified in the Principles. This Code of Conduct identifies good practices that should be adopted by providers, regardless of whether they are required under local regulation. The Code does not alter providers' responsibility to comply with local legal requirements. Similarly, the Code is not intended to limit or otherwise affect providers' contractual rights.

Principles

Principle 1: Mobile money providers ("providers") safeguard customer funds against risk of loss.

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

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 ("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 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

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

1.2.2 Providers shall regularly reconcile transactions and settle balances with financial ecosystem partners.[3]

3. For the purposes of the Code, "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). These entities would typically connect to the mobile money service via Application Programming Interfaces (APIs).

Principle 2: Providers have in place effective, proportional risk-based mechanisms to prevent, detect, and report the misuse of services for the purpose of money laundering or terrorist financing (ML/TF).

2.1 Effective policies and procedures

2.1.1 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

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

2.3 Appointed AML/CFT manager

2.3.1 Providers shall appoint a qualified employee to promote and monitor compliance with AML/CFT-related obligations.

2.4 Software to monitor transactions

2.4.1 Providers shall create a system to monitor transactions for AML/CFT purposes.

2.5 Risk-based KYC requirements and transaction / balance limits

2.5.1 Providers shall properly identify clients and may use a risk-based KYC approach if permitted by local laws and regulations.

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

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.

2.6.3 Providers shall develop clear policies and processes for addressing staff and agent AML/CFT violations.

Principle 3: Providers screen, train, and monitor staff, agents and entities providing outsourced services to ensure that they offer safe and reliable services and comply with all relevant operational and legal requirements.

3.1 Due diligence policies and procedures

3.1.1 Providers shall conduct proper due diligence on potential staff, agents and entities providing outsourced services.

3.2 Training

3.2.1 Providers shall develop and implement training programs for staff and agents.

3.3 Contractual agreements

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 and oversight

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

Principle 4: Providers have well-developed policies and processes and sufficient network and system capacity to ensure reliable service provision.

4.1 Board and senior management oversight

4.1.1 Providers shall ensure that the Board of Directors and senior management establish effective management oversight.

4.2 Service-level management and reporting

4.2.1 Providers shall develop and implement service-level monitoring and reporting systems.

4.3 Capacity management

4.3.1 Providers shall take steps to ensure sufficient network and system capacity through forecasting, monitoring, and testing.

4.4 Incident and problem management

4.4.1 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

4.5.1 Providers shall develop processes to ensure that systems and applications remain robust and secure following system and configuration changes.

4.6 Enterprise risk management

4.6.1 Providers shall establish a risk management framework for identifying, assessing, and controlling risks.

4.7 Business continuity

4.7.1 Providers shall develop effective business continuity and contingency plans.

Principle 5: Providers take robust steps to ensure the security of the mobile network and channel.

5.1 Security governance

5.1.1 Providers shall develop, implement, and regularly review a formal security policy for mobile money services.

5.1.2 Providers shall screen, train and monitor internal staff.

5.1.3 Providers shall ensure policies are in place for secure handling of information and assets.

5.1.4 Providers shall ensure protection of their assets that are accessible by suppliers and third parties.

5.2 Designing and developing secure systems, applications, and network

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 Ongoing security operations and fraud management

5.3.1 Providers shall identify and assess security risks prior to offering mobile money services and shall continue to monitor such risks on an ongoing basis.

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.

5.3.10 Providers shall develop risk-based policies and measures for fraud detection and prevention.

Principle 6: Providers communicate clear, sufficient, and timely information in a manner that customers can understand so that customers can make informed decisions.

6.1 Effective disclosure and transparency

6.1.1 Providers shall ensure that users are provided with clear, prominent, and timely information regarding fees and terms and conditions.

6.2 Safety and security

6.2.1 Providers shall educate customers on how to use mobile money services safely.

Principle 7: Providers have in place mechanisms to ensure that complaints are effectively addressed and problems are resolved in a timely manner.

7.1 Policies and procedures to ensure efficient resolution of customer complaints

7.1.1 Providers shall develop customer complaint policies and procedures.

7.1.2 Providers shall inform customers of the existence of customer complaint policies and procedures.

7.1.3 Providers shall develop specific policies for handling reversals.

7.2 Availability of customer service support

7.2.1 Providers shall provide an appropriate mechanism for customers to address questions and problems.

7.3 External recourse mechanisms

7.3.1 Providers shall specify how disputes can be resolved if internal resolution fails.

Principle 8: Providers follow good data privacy practices when collecting, processing, and/or transmitting customers' personal data.

8.1 Governance

8.1.1 Providers shall comply with good practices and relevant regulations governing customer data privacy.

8.2 Transparency and Notice

8.2.1 Providers shall ensure that users are provided with clear, prominent, and timely information regarding their data privacy practices.

8.3 User Choice and Control

8.3.1 Providers shall ensure that customers are informed of their rights and have opportunities to exercise meaningful choice and control over their personal information.

8.3.2 Providers shall seek customer consent for any changes that materially affect the privacy of their personal information.

8.4 Minimization of Data Collection and Retention

8.4.1 Providers shall limit the personal information that is collected from customers and is retained, used, or shared.

Annex: Definition of Mobile Money

For the purposes of the Code of Conduct, mobile money is a transformational service that uses information and communication technologies (ICTs) and non-bank retail channels to extend the delivery of financial services to clients who cannot be reached profitably with traditional branch-based financial services. Typical examples of mobile money services are e-wallets that are used to make person-to-person (P2P) transfers and a range of payments, or to receive salary and government-to-person (G2P) payments.

The key characteristics of a mobile money service are:

- Customers get money into and out of the service using a network of transactional agents that operate outside of bank branches; and
- Customers initiate transactions using an interface that is available on basic mobile handsets.

Although there is currently no standard regulatory definition of mobile money and electronic money (e-money) suitable for global use, countries that have developed their own definitions tend to include several common elements. Mobile money is monetary value that is:

- available to a user to conduct transactions through a mobile device;
- accepted as a means of payment by parties other than the issuer;
- issued upon receipt of funds;
- electronically recorded; and
- redeemable for cash.

In jurisdictions where e-money has been defined in regulation or legislation, mobile money is a form of e-money.

For further information please contact
mobilemoney@gsma.com
GSMA London Office
T +44 (0) 20 7356 0600