REGULATORY FRAMEWORK

FOR MOBILE PAYMENTS SERVICES

IN NIGERIA

Table of Content

1.0 Introduction

This regulatory framework is developed to conform to international best practice and standards. It is also a product of vigorous engagement and consultations with stakeholders.

After identifying person to person payments (over the mobile phone infrastructure) as a practical strategy for financial inclusion of the un-banked, the Central Bank of Nigeria opted for the creation of an enabling regulatory environment as a policy path towards achieving availability, acceptance and usage of mobile payments services in Nigeria.

The overriding vision is to achieve a nationally utilised and internationally recognised payments system.

1.1 Objectives

The objectives of the regulatory framework are as follows:

- Provision of an enabling environment for mobile payments services in reducing cash dominance in the Nigerian economy.
- Specification of minimum technical and business requirements for various participants in the mobile payments services industry in Nigeria.
- Stipulation of roles and responsibilities of participants in the provision and usage of mobile payments services in Nigeria.
- Provision of broad guidelines for implementation of processes and flows of mobile payments transactions from initiation to completion.

1.2 Scope

This regulatory framework addresses business rules governing the operation of mobile payment services in Nigeria. It specifies basic functionalities expected of any mobile payment service and solution in Nigeria. In addition, it

sets the basis for regulation of mobile payments services offered at different levels and by diverse participants. This framework does not cover the use of mobile phone as an access to the internet for the purpose of using internet banking services. In that regard, the provisions of the Electronic Banking Guidelines should apply.

1.3 Participants

The framework shall guide the activities of participants in the provision of mobile payments services. Participants include service providers, infrastructure providers, solution providers, scheme operators and the consumers.

1.3.1 Scheme Operators

Organizations that provide the infrastructure for the mobile payment systems for the use of participants that are signed-on to their scheme..

1.3.2 Settlement Infrastructure Providers

Organizations providing infrastructure that enables message exchange, switching and settlement facilities for mobile payments services.

1.3.3 Service Providers

Organizations that employ the infrastructure of scheme operators to provide mobile payments services to end users.

1.3.4 Consumers

These are end users of mobile payments services.

1.3.5 Solution Provider

These are information technology software developers that develops mobile payments software, application and other ancillary hardware.

2.0 Mobile Payment System

Mobile Payment System in Nigeria refers to the various components required to deliver mobile payment to the banking and non-banking community. The providers of these services and solutions shall be required to operate within the defined regulatory framework specified in this document.

The Central Bank of Nigeria shall be responsible for defining, monitoring and regulating the mobile payment systems in Nigeria.

2.1 Mobile Payment Models

This framework has identified three major models for the implementation of mobile payments services namely;

- Bank –Focused- Financial Institutions as Lead Initiator
- Bank Led – Financial Institution(s) and/or its Consortium as Lead Initiator
- Non-Bank Led- A corporate organisation as Lead Initiator

The Lead initiator shall be responsible for ensuring that the various solutions and services within a mobile payment system meet the entire regulatory requirement as defined by the Central Bank of Nigeria. The Lead initiator (as an entity and as representative of other partners) shall be legally responsible and accountable to the Central Bank of Nigeria and the end user.

The Central Bank of Nigeria appreciates the critical role of telecommunication companies in any of the models for the implementation of mobile payments services in Nigeria. The role of the telecommunication companies shall be guided by the following provisions;

Telecommunication companies shall

- provide telecommunication network infrastructure for the use of scheme operators;

- ensure that a secure communication path based on the technology standard stipulated in this regulatory framework is implemented;
- make available its network to scheme operators based on criteria which are transparent and generally applicable to all scheme operators without discriminatory practices against any scheme;
- ensure that its subscribers are free to use any mobile payments system service of their choice;
- not receive deposit from the public except in respect of the prepaid airtime billing of their subscribers
- not allow the use of the prepaid airtime value loaded by their subscribers for purposes of payment or to transfer monetary value.

2.1.1 Bank-Focused Model

This is a model where a bank delivers banking services to existing and prospective bank customers using the mobile phone as a delivery channel. This model can only be deployed by a licensed deposit-taking financial institution. Licensed deposit-taking financial institutions, under this model shall include, deposit money banks, microfinance banks and discount houses.

2.1.1.1 The Participants

The participants in this model shall include the initiating bank, its Information and Communication Technology (ICT) partners and the customers.

2.1.1.2 Responsibilities of the Financial Institutions

Financial Institutions shall be responsible for;

2.1.1.2.1 seeking and obtaining necessary approvals from the regulatory authorities.

2.1.1.2.2 the deployment and delivery of the mobile payment solutions to the customer

2.1.1.2.3 ensuring that the mobile payment solution meets all specified mobile payment standards as stated in the mobile payment services regulatory framework

2.1.1.2.4 putting in place adequate measures to mitigate all the risks that could arise from the deployment and use of its mobile payment solution.

2.1.1.2.5 facilitating international remittances to both scheme and non–scheme recipients.

2.1.1.3 Rules

The financial institutions shall ensure that

2.1.1.3.1 the mobile payment system meets all regulatory requirements and standards

2.1.1.3.2 it adheres to the requirements of the mobile payment KYC guidelines.

2.1.1.3.3 it makes adequate provision for monitoring and reporting as defined in the mobile payment monitoring and compliance guidelines.

2.1.1.3.4 remittance messages shall, at a minimum, be conveyed to the recipient through secured SMS.

2.1.2 Bank Led Model

This is a model where a bank, or a consortium of banks, partnering with other organizations, jointly seeks to deliver banking services leveraging on the mobile banking system.

This model shall be applicable only in a scenario where there exists collaboration between a licensed deposit-taking financial institution(s) and an organization duly verified by the partner bank(s). Licensed deposit-taking financial institutions, under this model shall include, deposit money banks, microfinance banks and discount houses.

2.1.2.1 The Participants

The participants in this model are the initiating bank(s), the partner organizations (e.g scheme operator, infrastructure providers telecommunications companies, independent operators etc) and the customers.

2.1.2.2 Roles of the Financial Institutions

The Financial Institutions shall:

2.1.2.2.1 provide all financial services for the operation of the mobile payments service.

2.1.2.2.2 verify, approve and guarantee the creditability and integrity of the partner organization.

2.1.2.3 Roles of the Partner Organizations

Among other roles as may be defined in the agreement with the financial institution(s), the partner organizations shall:

2.1.2.3.1 provide and manage the technology required to deliver mobile payment services to the customer

2.1.2.3.2 provide the agent network required to extend all the proposed services to the market place.

2.1.2.3.3 facilitate international remittances to both scheme and non –scheme recipients

2.1.2.4 Responsibilities of the Financial Institutions

The Financial Institutions shall be responsible for:

2.1.2.4.1 seeking and obtaining approval from the CBN;

2.1.2.4.2 providing financial, clearing and settlement services to the mobile payment system;

2.1.2.4.3 ensuring that the mobile payment solution complies with specified mobile payment standards as stated in the mobile payment services regulatory framework;

2.1.2.4.4 putting in place adequate measures to mitigate all the risks that could arise from the deployment and use of its mobile payment solution and;

2.1.2.4.5 educating the customers on the appropriate use of the solution;

2.1.2.4.6 recruiting, training, and managing the agents

2.1.2.5 Responsibilities of the Partner Organizations

The Partner organisations shall be responsible for:

2.1.2.5.1 ensuring that the proposed solution meets all the regulatory standards and requirements specified in the mobile payment services regulatory framework;

2.1.2.5.2 the deployment and delivery of the mobile payment solutions to the customer;

2.1.2.5.3 providing the agent network required to support the delivery of services to the customer;

2.1.2.5.4 collaborate with the financial institutions in recruiting, managing and training the agents on the network;

2.1.2.5.5 educating the customers on appropriate use of the solution;

2.1.2.5.6 ensuring that international remittance messages shall, at a minimum, be conveyed to the recipient through secured SMS.

2.1.2.6 Rules

2.1.2.6.1 The mobile payment system must meet all regulatory requirements and standards

The financial institution shall ensure that

2.1.2.6.2 it adheres to the requirements of the mobile payments KYC guidelines.

2.1.2.6.3 it makes adequate provision for monitoring and reporting as defined in the mobile payment monitoring and compliance guidelines.

2.1.2.6.4 international remittance messages shall, at a minimum, be conveyed to the recipient through secured SMS.

2.1.3 Non-Bank Led Model

This model allows a corporate organisation that has been duly approved by CBN to deliver mobile payments services to consumers. This model shall be applicable to any organization other than a licensed deposit money bank and telecommunication companies. Corporate organisation, under this model, include switching companies and payments system service providers.

2.1.3.1 The Participants

The participants in this model are the corporate organization, its partners and the consumers.

2.1.3.2 Roles of the Organization

2.1.3.2.1 The corporate organization would provide and manage the technology required to deliver mobile payment services to the customer.

2.1.3.2.2 The corporate organization would provide the agent network required to extend all the proposed services to the market place.

2.1.3.3 Responsibilities of the Organization

The organisation shall be responsible for:

2.1.3.3.1 ensuring that the proposed solution meets all the regulatory standards and requirements specified in the mobile payment services regulatory framework.

2.1.3.3.2 the deployment and delivery of the mobile payment solutions to the customer.

2.1.3.3.3 developing the agent network required to support the delivery of services to the customer.

2.1.3.3.4 recruiting, managing and training the agents on their network.

2.1.3.3.5 educating the customers on appropriate use of the solution

2.1.3.3.6 ensuring that its mobile payment system provides transactions monitoring and reporting system in compliance with regulatory requirements.

2.1.3.3.7 providing access for on-the-spot assessment and verification of its transaction details by the Central Bank of Nigeria on an on-demand basis.

2.1.3.3.8 providing a quarterly assessment report on the performance of the organization and the submission of same at the Banking Operations Department of the Central Bank of Nigeria.

2.1.3.3.9 keeping records of transaction details emanating from the organization's mobile payment system.

2.1.3.3.10 ensuring that the mobile payment solution complies with specified standards as stated in the regulatory framework.

2.1.3.3.11 putting in place adequate measure to mitigate all the risk that could arise from the deployment and use of its mobile payment solution.

2.1.3.3.12 shall appoint and notify CBN of its settlement bank among the CBN approved settlement banks.

2.1.3.3.13 facilitate international remittances to both scheme and non –scheme recipients.

2.1.3.4 Rules

The organisation shall ensure that:

2.1.3.4.1 monetary values in respect of its mobile payments services are reflected in the settlement bank financial system by maintaining a settlement account with a deposit money bank.

2.1.3.4.2 The settlement account with the deposit money bank shall be opened as a nominee account with users of the e-money issued on it as beneficiaries.

2.1.3.4.3 The settlement account is not interest bearing to both the users and the organisation

2.1.3.4.4 The settlement account is not used, under any guise or purpose, as collateral for negotiation of loans by the organisation.

2.1.3.4.5 The balance on the settlement account shall always be equal to the total outstanding (un-spent) balance of all holders of the e-money

2.1.3.4.6 the mobile payment system meets all regulatory requirements and standards

2.1.3.4.7 it adheres to the requirements of the mobile payments Know Your Customer (KYC) guidelines.

2.1.3.4.8 all customer transactions are traceable; auditable and can be validated.

2.1.3.4.9 international remittance messages shall, at a minimum, be conveyed to the recipient through secured SMS.

2.2 Types of Mobile Payments Scenarios

Mobile payment scenarios are methods through which mobile payments can be carried out. These scenarios could be;

- Card Account Based
- Bank Account Based
- Stored Value (e-Money) Account Based

2.2.1 Card Account Based

This is a scenario where a payment card is linked to a mobile phone for the purpose of initiating and concluding payment transactions.

2.2.1.1 Types of Card-Driven Payments

The types of card-driven payments recognized by the CBN are:

- Credit,
- Debit and
- Pre-Paid

2.2.1.2 Rules of Operations

2.2.1.2.1 The Card Account Based payment shall be based on an infrastructure that relies on the global 3-DES secure architecture.

2.2.1.2.2 The card shall be issued by a CBN approved card issuing organization

2.2.1.2.3 The card shall be recognized within the existing financial system

2.2.1.2.4 The card system shall comply with the existing regulation and standards for cards.

2.2.1.2.5 All Card Account based transactions must be authenticated against the originating Card Management System.

2.2.2 Bank Account-Based

This is a scenario where a mobile payment system drives transactions through bank accounts of customers. These accounts are based on the existing account-generating system in the banking system.

Some of the account type include: current account, saving account, domiciliary accounts etc.

2.2.2.1 Types of Bank Account Based

The types of Bank Account based scenarios shall include but not limited to Pull Based account transactions and Push Based account transactions.

The Pull-based transactions are transactions that generate a debit on the account through a mobile payment solution, whilst a Push-based generates a credit transaction through a mobile payment solution on the account. A Pull-based transaction shall be authorised by the account holder via a verifiable mode before the transaction is consummated and debited to his or her account.

2.2.2.2 Rules of Operations

2.2.2.2.1 The Bank Account Based payment shall be originated via a financial institution's banking application.

2.2.2.2.2 The Bank Account Based shall comply with the existing account opening standards and practice in the Nigerian banking system.

2.2.2.2.3 The transaction activities generated within/by the account shall be traceable, monitored and logged within the mobile payment system

2.2.2.2.4 Access to the account through the mobile payment system shall be via a secured mobile payment system that meets the defined standards specified in the mobile payment services regulatory framework.

2.2.2.2.5 Authorization of transactions originating from or terminating on these accounts shall be based on standards defined by the host financial institution.

2.2.3 Stored Value Account Based

This is a scenario where a mobile payment system drives transactions through a system-based account. These system-based accounts shall comply with the standards defined within the regulatory framework.

2.2.3.1 Type of Stored Value Account

The various stored value options recognized by the CBN include Re-loadable stored value accounts, prepaid account etc.

2.2.3.2 Rules of Operations

2.2.3.2.1 All system-based accounts shall have an identification system that generates unique identifier per user account within the mobile payment system.

2.2.3.2.2 All system-based accounts shall only be accessible through the mobile payment system.

2.2.3.2.3 The user may however specially request other means of access to his/her system-based account other than specified in 2.2.3.2.2 above. The liability of the user shall be clearly stated before granting request.

2.2.3.2.4 All accounts and transaction details shall be stored in an encrypted format within the mobile payment system.

2.2.3.2.5 The mobile payment system account management unit shall comply with all the standards and requirements defined in the mobile payment regulatory framework.

2.2.3.2.6 All system based stored value account shall be tied to a settlement account with a licensed deposit taking institution. The settlement account shall be funded to the tune of the total outstanding balance amount of all the system-based accounts on the scheme

2.3 Mobile Payment Processes

The mobile payment solution providers shall provide a detailed payment management process that covers the entire solution delivery process from customer registration and management, customer service and dispute resolution procedures to transaction settlement finality.

These processes shall cover the scope of the value chain across all the participants in the mobile payment system.

2.3.1 Operational Modalities

The Mobile Payment system shall support the following key processes for delivering payments to the customers through their handsets.

2.3.1.1 Registration

2.3.1.1.1 All scheme operators shall be registered with the Central Bank of Nigeria and shall be issued a unique scheme code by the national switch for managing interoperability within the national mobile payment system.

2.3.1.1.2 The mobile payment system deployed by a service provider shall have the capabilities to register all users within the payment system.

2.3.1.1.3 The service provider shall register users of its solution based on technology standards and requirement in this regulatory framework

2.3.1.1.4 The solution provider shall ensure that the registration processes within its mobile payment system shall fulfil the entire KYC requirement specified within the regulatory framework.

2.3.1.1.5 All mobile payment system users shall retain and maintain evidence of the successful completion of the registration process with a solution provider.

2.3.1.2 Activation

2.3.1.2.1 The mobile payment system shall require a registered user to activate the service before commencement of transactions with his PIN/Password.

2.3.1.2.2 The activation of service shall ensure that user identity is not compromised within or without the mobile payment system.

2.3.1.2.3 The activation of users shall be securely managed within the solution provider mobile payment system

2.3.1.2.4 The scheme operators shall ensure that the activation process is not compromised or altered within its infrastructure.

2.3.1.3 Transactions

2.3.1.3.1 All transactions initiated and concluded within the mobile payment system shall have a unique transaction reference issued by the system

2.3.1.3.2 All transactions shall have the following elements: Transaction number, transaction amount, transaction date and time stamps, merchant categories, merchant addresses and codes

2.3.1.3.3 Each transaction detail logged within the payment system shall contain a valid description, payer and payee phone numbers.

2.3.1.3.4 Mobile payment solution providers shall provide notifications for all transactions concluded on their mobile payment systems.

2.3.1.3.5 Scheme Operators shall ensure that all transactions processed within its infrastructure are not compromised.

2.3.1.4 Settlement

2.3.1.4.1 The settlement process to be deployed by scheme operators shall ensure compliance with the settlement standards and requirements defined in the mobile payment regulatory framework.

2.3.1.4.2 The scheme operator shall ensure that its mobile payment infrastructure fully complies with the mobile payment services regulatory framework requirement for finality of settlement.

2.3.1.4.3 The scheme operator shall provide all solution providers with settlement positions for reconciliation of transactions.

2.3.1.4.4 All final settlement processes shall be routed through the inter-bank settlement system.

2.3.1.4.5 The scheme operator shall ensure that all settlement information details are preserved for reference over a 5 year period.

3.0 Infrastructure

The core infrastructure in providing a national mobile payment system comprises transaction, clearing and settlement arrangements. These infrastructures consist of service providers, network facilities, information and computer technologies, operating procedures and rules. To achieve finality of payments to all parties, the settlement process for all models need to be defined as well as the rules guiding the various services.

Infrastructure already exists at the national switch and inter-bank settlement system, to facilitate the settlement finality of payment through the CBN Inter-Bank Funds Transfer System (CIFTS) infrastructure. Infrastructure shall facilitate instant payment to the end users and settlement of the Scheme providers in a T+1 cycle for the mobile payment system. The rules and regulation to provide such an operation are detailed below.

3.1 Settlement

There are various settlements processes which will come into place depending on how the mobile services were consummated. The services include Intra-Scheme (*On us; Not on us)* and Inter-Scheme (*On Us; Not On Us*).

3.1.1 Intra Scheme

Intra-Scheme Services are services that are consummated within a particular service provider's scheme. However, as there are various participants in each scheme, a service initiated by a particular participant on itself is referred to as a *On Us* service while a service initiated from one participant to another within the same scheme is referred as a *Not On Us*.

The role of Intra-Scheme Settlement Providers shall be to provide a net position of all their participants to the inter-bank settlement system to effect finality of payment.

3.1.2 Inter Scheme

Inter-Scheme Services are services consummated across two different schemes by various participants. When a service is consummated by the same participant that belongs to two different schemes, this service is referred to as *On Us* service. *Not On Us* service are services consummated by two different participants that belong to two different schemes.

The role of Inter-Scheme Settlement Providers shall be to provide a net position of all participants which consummate services across schemes to the inter-bank settlement system to effect the finality of payment.

3.1.3 Final Settlement

For finality of Settlement between participating institutions, settlement providers shall provide settlement information of their participants to the final settlement system. Final Settlement shall be done through the CBN Inter-Bank Funds Transfer System (CIFTS) by effecting the net positions of both the inter scheme and the intra schemes (Not on Us) provided by the national central switch and the inter-bank settlement system.

3.1.4 Operating Rules

3.1.4.1 Intra-Scheme (Not on Us) Settlement

Any organization providing intra-scheme settlement shall:

3.1.4.1.1 obtain CBN approval for the operation of the scheme.

3.1.4.1.2 maintain a settlement account with a bank that is a participant on CIFTS.

3.1.4.1.3 provide net settlement positions of all their participants to the participating banks for final settlement on a T+1 cycle.

3.1.4.1.4 provide statistical reports to the Regulators and participants as required.

3.1.4.1.5 maintain audit trail and transaction log of all transactions consummated on the scheme.

3.1.4.2 Inter Scheme Settlement

Any organization providing inter-scheme settlement shall:

3.1.4.2.1 provide net settlement positions of all Inter-Scheme service providers and effect final settlement using the CBN Inter-Bank Funds Transfer System (CIFTS) on (T+1) cycle.

3.1.4.2.2 provide statistical reports to the regulatory bodies and participants as required

3.1.4.2.3 maintain audit trail and transaction log of all transactions consummated on the scheme.

3.1.5 Roles and Responsibilities

3.1.5.1 Intra Scheme Settlement

Any organization providing intra-scheme settlement shall:

3.1.5.1.1 provide the infrastructure (hardware, software, switching and security) to participating service providers on mobile payments schemes.

3.1.5.1.2 provide business continuity and disaster recovery plans to ensure services are always available at all times.

3.1.5.1.3 provide 99.99% system availability and ensure all signed on participating institutions follows same rule.

3.1.5.1.4 ensure all infrastructures are interoperable across all providers.

3.1.5.2 Inter Scheme Settlement

Any organization providing inter-scheme settlement shall:

3.1.5.2.1 provide the infrastructure (hardware, software, switching and security) to link all inter scheme providers.

3.1.5.2.2 provide business continuity and disaster recovery plans to ensure services are always available at all times.

3.1.5.2.3 provide 99.99% system availability and ensure that all signed-on participating institutions follow same rules.

3.1.5.2.4 ensure that all infrastructures are interoperable across all providers.

3.2 Scheme Operators

Scheme Operators provide the infrastructure for the mobile payment systems for the use of participants that are signed-on to their scheme.

3.2.1 Participants

The participants in this industry are Banks, Payments Switches and Independent Scheme Operators.

3.2.2 Operating Rules

For any of the following interested parties to operate as scheme operator they shall adhere to the following rules:

3.2.2.1 Banks

Banks shall:

3.2.2.1.1 obtain CBN approval before operating the scheme

3.2.2.1.2 have systems to provide KYC information to all regulatory bodies

3.2.2.1.3 ensure that independent service providers pledge adequate collateral where it provides settlement banking relationship.

3.2.2.1.4 ensure that the settlement accounts of the independent service providers to which it provides banking services is drawn down by only the net settlement position of the provider.

3.2.2.2 Payment Switches

Payments switches shall:

3.2.2.2.1 obtain CBN approval to operate the scheme

3.2.2.2.2 maintain systems to provide KYC information to all regulatory bodies

3.2.2.2.3 ensure that service providers utilizing their infrastructure provides adequate collateral to mitigate settlement risk.

3.2.2.3 Independent Scheme Operators

Independent scheme operators shall:

3.2.2.3.1 obtain CBN approval to operate the scheme

3.2.2.3.2 maintain systems to provide KYC information to all regulating bodies

3.2.2.3.3 ensure that service providers utilizing their infrastructure provide adequate collateral to mitigate settlement risk.

3.2.3 Roles and Responsibilities

Scheme operators shall:

3.2.3.1 provide the infrastructure (hardware, software, switching and security) to participating service providers on mobile payments.

3.2.3.2 provide business continuity and disaster recovery plans to ensure services are always available at all times.

3.2.3.3 provide 99.99% system availability and ensure all signed on participating institutions follow same rule.

3.2.3.4 ensure all infrastructure are interoperable across all providers

3.3 Service Providers

The service providers employ the infrastructures of the Scheme Operators to provide services to the end users.

3.3.1 Participants

The participants in this industry are Banks, Telecommunication Companies, and Independent Service Providers.

3.3.2 Operating Rules

For any of the following interested parties to operate as service providers they shall abide by the following rules:

3.3.2.1 Banks

The banks shall:

3.3.2.1.1 obtain CBN approval to provide the service

3.3.2.1.2 provide KYC information to all regulatory bodies

3.3.2.1.3 provide adequate collateral to mitigate settlement risk

3.3.2.2 Independent Service Providers

The independent service providers shall:

3.3.2.2.1 obtain CBN approval to provide the service

3.3.2.2.2 provide KYC information to all regulatory bodies

3.3.2.2.3 provide adequate collateral to mitigate settlement risk

3.3.2.2.4 maintain a settlement account with a settlement bank

3.3.2.2.5 ensure that all payments for purchases of issued stored value are made into designated settlement account.

3.3.3 Roles and Responsibilities

Service providers shall:

3.3.3.1 provide customer support service

3.3.3.2 provide users with user manuals and training in using the scheme.

3.3.3.3 have procedures for efficient dispute resolution.

3.3.3.4 guarantee that the mobile payment system will be available 99.99%

3.3.3.5 maintain details of transaction records consummated within their mobile payment system for 5 years

3.3.3.6 ensure that the customer gets the notification for every transaction on its mobile and an alternative medium e.g e-mail.

3.3.3.7 ensure compliance with the standards and requirements of the mobile payment system guideline.

3.3.4 Risk Management for Independent Service Providers

In view of the peculiarity of the operations of the independent service providers and the unique risks associated with their operations, the regulatory framework hereby specifies the following requirements to mitigate risks arising from the activities of the independent service providers.

3.3.4.1 Credit and Settlement Risk

Independent service providers shall:

3.3.4.1.1 ensure that the mobile payment system automatically generates settlement information.

3.3.4.1.2 ride on the capabilities of the scheme operators for settlement purposes.

3.3.4.1.3 maintain audit trail and settlement log for 5 years.

3.3.4.1.4 maintain a minimum paid-up capital of N20million unimpaired by losses

3.3.4.1.5 fulfill other conditions that may be specified by the regulatory authorities from time to time.

3.3.4.2 Business Continuity Risk

Independent service providers shall:

3.3.4.2.1 maintain proper backup infrastructure

3.3.4.2.2 implement a disaster recovery and business continuity plan

3.3.4.2.3 periodically test the effectiveness of the backup infrastructure and business continuity plan.

3.3.4.3 Other Risks

Independent service providers shall:

3.3.4.3.1 implement a robust risk management framework to identify, monitor and control all other risks that may arise out of the operation.

3.3.4.3.2 ensure that ownership is credible and the top management is experienced.

3.3.4.3.3 be registered with CAC as Limited Liability Company.

4.0 Technology

The technology implemented for mobile payment services shall comply with the following technology standards and other requirements outlined in the provisions of this regulatory framework.

4.1 Standards

4.1.1 Modularity of Technologies

4.1.1.1 The technology deployed in the delivery of mobile payment services shall comprise a set of interoperable infrastructure modules that work seamlessly. There shall be an end-to-end connection from user-device through transport network to the service site.

4.1.1.2 Provided the security requirements of this regulatory framework are met, the mobile payment service shall use any mode of communication including, but not restricted to, the following:

Secure SMS,

WAP/GPRS and

USSD1

EDGE

4.1.1.3 Provided the security requirements of this framework are met, the mobile payments service shall use any mode of user interface, including, but not restricted to, the following :

Secure SMS

Menu driven USSD1 application

WAP/GPRS

4.1.1.4 The mobile payments services shall not use plain SMS.

4.1.1.5 Only secure channels shall be used in providing mobile payments services

4.1.1.6 The mobile payments services shall ensure non-repudiation

4.1.1.7 The mobile payment solution may be embedded into SIM toolkit. The NCC shall stipulate standards for all telecommunication network service providers to facilitate embedding of mobile payment solutions.

4.1.2 Solution Initialisation

The mobile payments solution shall ensure simple initialization of the payment application.

4.1.3 Compatibility

4.1.3.1 The mobile payment solution shall be compatible and interoperable with the network infrastructure of different telecommunication companies, solution providers, and scheme providers and the Nigeria Central Switch.

4.1.4 Interoperability

All schemes shall be able to interoperate:

4.1.4.1 with other scheme or solution providers

4.1.4.2 with other payment channels like cards, ATM, POS, etc.

4.1.4.3 with the National Central Switch

4.1.4.4 The National Central Switch shall provide scheme codes for the various operators of mobile payments services for the purpose of seamless operations and settlements, with the ultimate aim of giving immediate value to all user transactions.

4.1.5 Message Format

Mobile Payments solutions deployed shall adhere to the following message format:

4.1.5.1 encrypted end-to-end

4.1.5.2 ISO 8583 compliant.

4.1.6. Reliability

4.1.6.1. Payment instruction shall be consistently executed. In the event of failure, immediate reversal shall be automatic.

4.1.6.2 Users shall get immediate value for every successful transaction.

4.1.7 Flexibility

Users shall be able to switch between service providers without any bottlenecks. Switching from one solution to another shall be as easy as possible.

4.1.8 User Interface

4.1.8.1 The user interface shall, at the minimum, be menu-driven.

4.1.8.2 If private or personal data in the application are directly accessible through this menu (for example, memorizing the PAN-Primary Account Number), the access to this menu shall be protected.

4.1.8.3 Administrative functions - for example, tracing, certification/confirmation of transaction shall be provided.

4.1.8.4 PIN shall be encrypted at the point of entry.

4.1.9 Security

The overall security framework shall ensure:

4.1.9.1 encrypted messaging / session between consumer's phone and third party service provider / Telecom Company. The minimum encryption standard to be specified is Triple Data Encryption Standard (3-DES) encryption;

4.1.9.2 all subsequent routing of messages to the scheme providers' servers must be with the highest level of security with dedicated connectivity like leased lines (E1 links) / VPNs;

4.1.9.3 that Hardware Security Module (HSM) exists between Nigeria Central Switch, service providers and all financial or third party institutions that participate in the scheme;

4.1.9.4 that any sensitive information stored in third party systems is restricted with appropriate encryption and hardware security standards;

4.1.9.5 all transactions on an account shall be allowed only after authentication of the mobile number and the PIN associated with it;

4.1.9.6 that mobile payments application shall not allow the option of saving the PIN either on the handset or on the application;

4.1.9.7 all accounts activated by the consumer on the mobile application is linked to the mobile phone number. This mobile number shall be used as the second factor authentication for mobile transactions;

4.1.9.8 the PIN does not travel in plain text during the transaction;

4.1.9.9 that proper system of verification of the phone number shall be implemented;

4.1.9.10 the payment authorisation message from the user's mobile phone shall, at the minimum, be triple DES encrypted and checked for tampering by the service or scheme provider. It shall not be possible for any interceptor to change the contents of the message;

4.1.9.11 existence of a security policy duly approved by the Board of Directors of the organisation providing the service.

4.1.9.12 segregation of duty of Security Officer / Group dealing exclusively with information systems security and Information Technology Division which actually implements the computer systems;

4.1.9.13 that Information Systems Auditor audits the information systems;

4.1.9.14 logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. exists;

4.1.9.15 at the minimum, the use of proxy server type of firewall so that there is no direct connection between the Internet and the scheme providers' systems. For sensitive systems, a stateful inspection firewall shall be implemented to thoroughly inspects all packets of information, compare past and present transactions and enable a real time security alert;

4.1.9.16 the information security officer and the information system auditor undertake periodic penetration tests of the system, which shall include;

- Attempting to guess passwords using password-cracking tools;
- Search for back door traps in the programs;
- Attempt to overload the system using DDoS (Distributed Denial of Service) & DoS (Denial of Service) attacks;
- Check if commonly known holes in the software, especially the browser and the e-mail software exist;
- regular penetration testing on the mobile payment system;

4.1.9.17 physical access controls is strictly enforced. Physical security shall cover all the information systems and sites where they are housed, both against internal and external threats.

4.1.9.18 proper infrastructure and schedules for backing up data. The backed-up data shall be periodically tested to ensure recovery without loss of transactions in a time frame as given out in the security policy.

4.1.9.19 the existence of disaster recovery sites and regular testing of its facilities for the purpose of business continuity.

5.0 Business Rules

5.1 E-Money

E-Money is monetary value stored electronically in a centrally held electronic device. It shall possess the following characteristics to be classified as e-money:

- issued on receipt of funds
- accepted as a means of payment by parties other than the issuer
- its value shall be transferable
- shall have defined cash out capabilities
- e-money is not entitled to any interest payments
- charges are not allowed on e-money floats

5.1.1 Issuers

The issuer is the entity which receives payment in exchange for value distributed in the system and which is obligated to pay or redeem transactions or balances presented to it. The issuer of e-money can either be a bank or a third party with the necessary authorization/license from the regulatory authorities.

5.1.1.1 Bank Issuer

This is the institution that pledges the float. They are responsible for

5.1.1.1.1 settlement of all transactions against (all) their e-money schemes

5.1.1.1.2 appointment of Agents and subagents

5.1.1.1.3 monitoring the exit of agents and sub-agents

5.1.1.1.4 ensuring compliance to KYC/AML limits as set

5.1.1.1.5 enrolment of customers

5.1.1.1.6 sale of e-money

5.1.1.1.7 cash out/withdrawal

5.1.1.1.8 complying with the minimum technical specification for the operation of this scheme as specified in this framework.

5.1.1.1.9 interoperability with other scheme operators

5.1.1.1.10 maintaining and providing the regulator with data on transactions on the mobile payments scheme detailing transaction volume and value on a weekly basis.

5.1.1.1.11 the provision of adequate collateral securities with the regulatory authority for the purpose of mitigating settlement risks. The amount shall be stipulated and reviewed by the regulatory authority as may be deemed necessary from time to time.

5.1.1.1.12 the replenishment of the pledge within 24 hours of depletion, failing which the issuer shall be sanctioned.

5.1.1.1.13 complying with all the provisions of this regulatory framework, failing which the regulator may mete out appropriate sanctions as may be deemed fit.

5.1.1.2 Non-Bank Issuer

The Non-bank issuers of e-money for the purpose of mobile payments are institutions, other than deposit money banks, who are responsible for:

5.1.1.2.1 the appointment of Agents and subagents

5.1.1.2.2 monitoring the exit of agents and subagents

5.1.1.2.3 ensuring compliance to KYC/AML limits as set

5.1.1.2.4 obtaining license from the regulatory authority for the operation of the scheme.

5.1.1.2.5 complying with the minimum technical specification for the operation of this scheme as specified in this framework.

5.1.1.2.6 interoperability with other scheme operators

5.1.1.2.7 maintaining and providing the regulatory authority with data on transactions on the mobile payments scheme detailing transaction volume and value on a weekly basis.

5.1.1.2.8 providing adequate collateral securities with the regulatory authority for the purpose of mitigating settlement risks. The amount shall be stipulated and reviewed by the regulatory authority as may be deemed necessary from time to time

5.1.1.2.9 replenishment of the pledge within 24 hours of depletion, else the issuer shall be sanctioned

5.1.1.2.10 maintaining a settlement account with one of the designated settlement banks for the purpose of settling inter-scheme settlement positions. The non-bank issuer shall notify the regulator of the settlement bank of its choice. The settlement account shall warehouse the total outstanding balance of e-money issued at any given time.

5.1.1.2.11 complying with all the provisions of this regulatory framework, failing which the regulator may mete out appropriate sanctions as may be deemed fit.

5.1.1.2.12 collaborating with other financial institutions to offer services to the tune of the limits specified for semi-banked in the KYC/AML section of this framework.

5.2 Agents Network

A contractual relationship in which one party, the agent, acts on behalf of another party, the principal. The agent may execute trades for the principal but is not responsible for performance by the principal.

5.2.1 Roles and Responsibilities of the banks and scheme operators to their agents are as follows:

Banks and scheme operators:

5.2.1.1 may appoint agents to facilitate the following activities in connection to their mobile payments services:

- Enrolment of customers
- Deposit
- Withdrawal /Cash-out

5.2.1.2 shall carry out the following due diligence before appointing an agent;

5.2.1.3 Where agent is an individual, the name, address, signature and/or finger prints of the agent shall be obtained and verified appropriately;

5.2.1.4 Where the agent is a corporate body or a registered business, the bank shall verify its registration and obtain the following documents:

- Copies of Certificate of Incorporation/Registration of Business
- Memorandum and Article of Association
- Board Resolution authorizing the organization to offer mobile payments agency services
- Any other relevant document for KYC/CDD purposes.
- List of Head Office and Operational offices/kiosks.

5.2.1.5 the agent shall be a customer of the bank and/or scheme operator and shall maintain a bank account with a bank in Nigeria.

5.2.1.6 shall be able to monitor the agent's cash-in-hand at all reasonable periods and evacuate same based on pre-agreed limits.

5.2.1.7 shall give an operational brochure detailing the expected process for each activity of the agents.

5.2.1.8 shall establish reasonable control procedures around the activities of the agent.

5.2.1.9 shall purchase a fidelity insurance cover for the activities of its agents.

5.2.1.10 shall maintain customer complaint/help line which shall be conspicuously displayed at the offices/kiosks of the agent.

5.2.1.11 shall ensure that all transactions consummated under its payment scheme has an industry standard audit trail.

5.2.1.12 shall maintain an online link to the agent.

5.2.1.13 shall ensure that its agents are well trained to deliver the services they offer

5.2.1.14 shall ensure that the agent displays its brand visuals conspicuously at all times

5.2.1.15 shall ensure that the relationship between it and its agents as well as the income derivable by the agents are documented and agreed.

5.2.2 Roles and Responsibilities of Agent

The agent shall:

5.2.2.1 maintain an account with the bank or scheme operators.

5.2.2.2 maintain a till not exceeding N100,000.00 at any time.

5.2.2.3 report any transaction he deems suspicious.

5.2.2.4 shall conspicuously display the complaint/help line maintained by the bank.

5.2.2.5 Effectively use the online link provided by the bank/e-money issuer in the conduct of his/her business

5.2.2.6 the agents are not restricted to any one scheme operator (They can serve as agents to multiple operators).

5.2.3 Know Your Customer (KYC) and Customer Due Diligence (CDD) Requirements

A hierarchical approach towards the implementation of KYC/CDD is required to make a success of financial inclusion strategy of mobile banking. A three-tiered KYC/CDD requirement matrix for mobile payments scheme provider is therefore stipulated as follows:

BANKING STATUS	KYC/CDD LEVEL	VERIFICATION REQUIREMENT	MOBILE PAYMENT TRANSACTION LIMIT
Un-banked	Least KYC	Name and Phone Number	Maximum transaction limit of N3,000 and Daily limit of N30,000
Semi-banked	Partial KYC	Refer to CBN KYC Manual and Money Laundering (Prohibition) Act.	Maximum transaction limit of N10,000 and Daily limit of N100,000
Fully-banked	Full KYC	Refer to CBN KYC Manual and Money Laundering (Prohibition) Act.	Maximum transaction limit of N100,000 and Daily limit of N1,000,000.

The above matrix shall apply to individuals while merchants as account holders shall be subjected to the full KYC requirements for corporates. Schemes operated by independent organisation shall not allow mobile payments transaction beyond the limit stipulated above for the un-banked.

5.2.4 Anti-Money Laundering Regulation

The mobile payments scheme operator shall notify the Nigeria Financial Intelligence (NFIU) of suspicious transactions. Suspicious mobile payments transaction shall be identified based on the following criteria:

5.2.4.1 Any single mobile payment (individual) account (including virtual and stored value account) which receives a total volume of payments of more than 100 in a day.

5.2.4.2 Any single mobile payment (merchant) account (including virtual and stored value account) which receives a total volume of payments of more than 1000 in a day.

5.2.4.3 Any single mobile payment (individual) account (including virtual and stored value account) which receives a total value of payments of ₦1m and above in a day.

5.2.4.4 Any single mobile payment (merchant) account (including virtual and stored value account) which receives a total value of payments of ₦10m above in a day.

The regulatory authorities reserve the right to change the criteria for suspicious transactions reporting in respect of mobile payments as it deemed fit. Such amendments shall be communicated by appropriate channel to the mobile payments scheme operators and other stakeholders.

5.3 Certainty of Mobile Transactions

For the purpose of establishing certainty of transactions through mobile payments, mobile payments scheme operators shall ensure the following:

5.3.1 Summary of transaction requested must be displayed to the user for confirmation. The transaction summary shall include, the phone numbers of the paying user and receiving user, transaction description, the transaction amount, date and time and a unique transaction identifier. By confirming the summary, the user commits to the transaction.

5.3.2 Option for the user to save such transaction summary.

5.3.3 Upon completion of the transaction, the user receives an electronic receipt which shall conform to the transaction summary earlier received and the option for saving the electronic receipt shall be available to the user.

5.3.4 The electronic summary of transaction and the electronic receipt should be securely logged and the log maintained online for a minimum period of three (3) months and subsequently archived for a minimum period of seven (7) years. However, if a complaint arises before the expiration of seven (7) years, the log in

respect of such pending complaints shall be maintained until the case is completely resolved or discharged.

5.3.5 The regulatory authority (or its agent) is granted access to the log when required for the purpose of certifying a printed copy for evidential purposes.

6.0 User Protection

6.1 Responsibilities of Mobile Payments Scheme Operators

6.1.1 Operators shall maintain a functional dispute and complaints resolution desk which shall be equipped to receive complaints through phone calls, e-mails and personal visit/contact from the user.

6.1.2 The addresses, telephone lines and e-mail of the complaint resolution desk must be well advertised through various media and at their agents' locations.

6.1.3 Operators and/or their agents shall be the first point of call for any subscriber of mobile payments scheme to register any complaint.

6.1.4 Mobile payments scheme operators shall ensure that complaints are acknowledged with a case identifier issued to the complainant within 24 hours and resolved within 3 working days of registering such complaints.

6.1.5 Operator shall ensure that all calls to the telephone lines of the dispute/complaint resolution desk should be recorded and maintained till the dispute is resolved.

6.1.6 Complaints by personal visits must be adequately logged with the name and signature (or thumbprint) of the complainant documented against the complaint.

6.1.7 Operators must ensure adequate due diligence in appointing agents as they shall be held accountable for the activity of their agents, if lapses are established against them in respect of their due diligence responsibilities.

6.1.8 Ensure consumer education and awareness to promote ease of use, security and adoption.

6.2 Rights of Users

6.2.1 Ease of enrolment

6.2.2 Easy to use (Menu Driven, SMS, USSD, etc)-maximum of 25 key strokes

6.2.3 Privacy, Trust and Security of transaction

6.2.4 Convenience: anywhere, anytime.

6.2.5 Accessibility to funds on completion of transaction process

6.2.6 Immediacy of transfer and value

6.2.7 Assurance of value to the recipients

6.2.8 Easy and prompt access to dispute resolution process

6.3 Responsibilities of Users

6.3.1 Ensure the protection of PIN / Password

6.3.2 Ensure prompt reporting of fraud cases / attempts, errors and complaints

6.3.3 Ensure proper confirmation of transaction details and recipients' mobile phone numbers at all times before authorizing transaction.

6.3.4 Comply with all security rules as provided by the scheme operator

6.3.5 Escalate complaints to the ombudsman through the offices of the Central Bank of Nigeria if resolution to complaints is unduly delayed.

6.4 Composition and Role of Ombudsman in Dispute Resolution

The Central Bank of Nigeria shall establish the Office of the Ombudsman. The Office of the Ombudsman shall comprise:

6.4.1 A representative of the Nigeria Communication Commission.

6.4.2 A representative of the Consumer Protection Council

6.4.3 A representative of scheme operators

6.4.4 A representative of financial institutions

6.4.5 An eminent professional or a respectable Nigeria

6.4.6 A member of the National Payments System Committee

6.4.7 The Central Bank of Nigeria

The roles of the Office of the Ombudsman shall be as follows:

6.4.8 Receive, investigate and resolve complaints involving all participants.

6.4.9 Sustenance of confidence in the mobile payments schemes.

6.4.10 Creation of an environment that encourages expeditious resolution of complaints.

6.4.11 Monitor and ensure instant compensation or otherwise notification to the complainant for decided cases.

6.4.12 Recommend improvement to mobile payments services.

6.4.13 Promote consumer education and awareness.

7.0 Compliance Monitoring

The Central Bank of Nigeria shall ensure the establishment of appropriate processes and procedures for the purpose of monitoring compliance to the regulatory framework.

Non-compliance with the provisions of this regulatory framework shall attract appropriate sanctions as may be determined by the Central Bank of Nigeria.

Glossary of Terms

1. **CIFTS**: The Real Time Gross Settlement (RTGS) System deployed by the Central Bank of Nigeria which effects settlement of transfer among banks on real time and gross basis. It is known as the CBN Inter-Bank Funds Transfer System (CIFTS).

2. **Financial Institution:** A deposit taking institution duly licensed by the Central Bank of Nigeria.

3. **Interoperability:** a situation in which payment instruments belonging to a given scheme may be used in systems installed by other schemes.

4. **Inter-Scheme Operation:** Inter-Scheme operations are mobile payments consummated across two different schemes by various participants.

5. **Intra-Scheme Operations**: Intra-Scheme operations are mobile payments that are consummated within a particular service provider's scheme.

6. **Issuer:** the entity which receives payment in exchange for value distributed in the system and which is obligated to pay or redeem transactions or balances presented to it.

7. **Scheme Operators** provide the infrastructure for the mobile payment systems for the use of participants that are signed-on to their scheme.

8. **Service Providers** employ the infrastructure of the scheme operator to provide services to end users.

9. **Settlement Infrastructure Providers** Organizations providing infrastructure that enables message exchange, switching and settlement facilities for mobile payments services.