CENTRAL BANK OF NIGERIA
Central Business District
P.M.B. 0187,
Garki, Abuja.
+234 - 0946238445

BANKING AND PAYMENTS SYSTEM DEPARTMENT

BPS/DIR/GEN/CIR/02/009 **September 9, 2015**

To: All Deposit Money Banks, Mobile Money Operators, and Payments Service Providers.

EXPOSURE DRAFT ON THE STANDARDS AND GUIDELINES ON ELECTRONIC CHANNELS OPERATIONS IN NIGERIA

The Central Bank of Nigeria (CBN), in furtherance of its mandate for the development of the electronic payments system in Nigeria hereby, releases the Exposure Draft on the Standards and Guidelines on Electronic Channels Operations in Nigeria for your review and comments.

Kindly forward your inputs on or before September 29, 2015 to the Director, Banking & Payments System Department and pspo@cbn.gov.ng.

Thank you for your usual cooperation.

'Dipo Fatokun
Director, Banking & Payments System Department

CENTRAL BANK OF NIGERIA

STANDARDS AND GUIDELINES ON ELECTRONIC CHANNELS OPERATIONS IN NIGERIA

STANDARDS AND GUIDELINES ON ELECTRONIC CHANNELS OPERATIONS IN NIGERIA

Sections/Table of Contents

Preamble

In exercise of the powers conferred on the Central Bank of Nigeria (CBN) by Section 47 (2) of the CBN Act, 2007 (as amended), to promote and facilitate the development of efficient and effective systems for the settlement of transactions, including the development of electronic payment systems; and

Pursuant to its inherent powers, the CBN hereby issues the following guidelines for Standards and Guidelines on Electronic Channels Operations in Nigeria.

1. GUIDELINES ON AUTOMATED TELLER MACHINE (ATM) OPERATIONS

1.1 The Standards

1.1.1 Standards on ATM Technology and Specification:

a. All ATM deployers/acquirers shall comply with Payment Card Industry Data Security Standards (PCIDSS).

b. All ATMs shall be able to dispense all denominations of Naira.

c. For deposit taking ATMs, acceptable denominations shall be displayed by the deployer.

d. All terminals shall be levels 1 & 2 EMV compliant at a minimum, and shall be upgraded from time to time to comply with the latest version within twelve months of release of the version.

e. All ATMs shall have audit trail and logs capabilities, comprehensive enough to facilitate investigations, reconciliation and dispute resolution.

f. Card readers shall be identified by a symbol that:

   i. represents the card;
   ii. identifies the direction for which the card should be inserted into the reader

g. 2% of ATMs deployed shall have tactile graphic symbol for the use of visually impaired customers. This should be complied with within five years from the release of these standards.

h. All new ATMs shall accept card horizontally with the chip upwards and to the right.

1.2 The Guidelines

ATM deployment

a. All Banks or independent ATM deployers may own ATMs; however such institutions must enter into an agreement with a card scheme or a scheme operator or their designated settlement agent for acceptance and settlement of all the transactions at the ATM.

b. All ATM transactions in Nigeria shall be processed by a Nigerian company operating in Nigeria as acquirer-processor.

c. No card or payment scheme or Card Association shall compel any issuer or acquirer to send any transaction outside Nigeria for purpose of processing, authorization or switching if the transaction is at an ATM or at any acceptance device in Nigeria and the issuer is a Nigerian bank or any other issuer licensed by the CBN.

d. All transactions at an ATM in Nigeria shall, where the issuer is a Nigerian bank or any other issuer licensed by the CBN be settled under a domestic settlement arrangement operated by a Nigerian Company. All collaterals for such transactions shall be in Nigerian National Currency and deposited in Nigeria.

e. No card scheme shall discriminate against any ATM owner or acquirer. Every card-scheme must publish for the benefit of every ATM owner or acquirer and the Central Bank of Nigeria the requirements for acquiring ATM transactions under the card scheme.

f. No ATM owner or acquirer shall discriminate against any card scheme or issuer.

g. Stand-alone or closed ATMs are not allowed.

h. ATMs should be situated in such a manner as to permit access at reasonable times. Access to these ATMs should be controlled and secured so that customers can safely use them.

i. Lighting should be adequate for safe access and good visibility. It should provide a consistent distribution and level of illumination, particularly in the absence of natural

light.

j. ATMs should be sited in such a way that direct or reflected sunlight or other bright lighting is prevented from striking the ATM display, for example, through the use of overhead sun shelter

k. Privacy shall be provided by the design and installation features of the ATM so that in normal use the cardholder does not have to conspicuously take any protective action.

l. All ATMs shall accept all cards issued in Nigeria under CBN regulations for any card-based value added service made available on the machine.

1.3 ATM Operations:

A bank or independent organization that deploys an ATM for the use of the public shall ensure that:

a. The ATM downtime (due to technical fault) is not more than seventy-two (72) hours consecutively, where this is not practicable, customers shall be duly informed by the deployer;

b. The helpdesk contacts are adequately displayed at the ATM terminals. At the minimum, a telephone line should be dedicated for fault reporting and such telephone line shall be functional and manned at all times that the ATM is operational.

c. All ATM charges are fully disclosed to customers;

d. The ATMs issue receipts, where requested by a customer, for all transactions, except for balance enquiry, stating at a minimum the amount withdrawn, the terminal identity, date and time of the transaction;

e. Receipt prints and screen display are legible. The dispensing deposit and recycling component of the machine is in proper working condition;

f. Cash retraction shall be disabled on all ATMs;

g. There is appropriate monitoring mechanism to determine failure to dispense cash; (Refer to the circular on Auto-Reversals)

h. There is online monitoring mechanism to determine ATM vault cash levels

i. ATM vault replenishment is carried out as often as possible to avoid cash-out.

j. ATMs are not stocked with unfit notes;

k. Availability of cash in the ATMs at all time. The funding and operation of the ATM deployed by non-bank institutions should be the sole responsibility of the bank or institutions that entered into agreement with them for cash provisioning. In this regard, the Service Level Agreement (SLA) should specify the responsibilities of each of the parties.

l. Change of PIN is provided to customers free of charge throughout the entire value chain.

m. Acquirers monitor suspicious transactions and report statistics to CBN based on the agreed format and timeframe

n. Back-up power (inverter) is made available at all ATM locations in such a way that the machine would not cease operation while in the middle of a transaction.

o. Waste disposal basket is provided at all ATM locations

p. A register of all their ATMs in Nigeria with location, identification, serial number of the machines, etc is maintained.

q. Provision is made for extending the time needed to perform a specific step by

presenting a question, such as, "Do you need more time?"

r. Information sufficient to construct a usable card is not displayed on the screen or printed on a transaction record. This will guard against the possibility that such information may become accessible to another person should the cardholder leave the ATM while a transaction is displayed, or abandon a printed transaction record.

s. Precautions are taken to minimise the possibility of a card being left by a message or voice alerting the customer to take his card.

t. Cash out first before card is out of the ATM is adopted to minimise the possibility of customers leaving cash uncollected at ATM.

u. ATM acquirers that disable cash-retract shall display such notice at the ATM or on the screen.

1.4 ATM Maintenance

A bank or independent organization that deploys an ATM for the use of the public shall ensure that:

a. Notice is displayed at the ATM for planned maintenance period and disruption to service due to maintenance for public;

b. An ATM maintenance register or log is kept properly

c. All ATMs and cash in the machines are insured.

d. They physically inspect their ATMs at least fortnightly.

1.5 ATM Security

a. Every ATM shall have cameras which shall view and record all persons using the machines and every activity at the ATM including but not limited to: card insertion,

PIN entry, transaction selection, cash withdrawal, card taking, etc. However, such cameras should not be able to record the key strokes of customers using the ATM.

b. Where a surveillance camera is used, it should be kept secretly to avoid thieves removing or damaging or compromising it.

c. Networks used for transmission of ATM transactions must be demonstrated to have data confidentiality and integrity

d. All ATMs must be located in such a manner that guarantees safety and security of users and confidentiality of their transactions.

e. ATMs should not be placed outside buildings unless such ATM is bolted to the floor and surrounded by structures to prevent removal.

f. Additional precaution must be taken to ensure that any network connectivity from the ATM to the bank or switch is protected to prevent the connection of other devices to the network point.

1.6 Dispute Resolution

In the event of irregularities in the account of an ATM customer arising from the use of card on ATM, the following shall apply:

a. All cardholders' complaints should be treated within a maximum of 72 hours from the date of receipt the complaints.

b. Where records are falsified by any party, adequate sanctions shall apply.

1.7 Liability Shift

a. Where a non EMV card is used on a non EMV Terminal and a fraud occurs, liability is on either the Card Issuer or the Card Holder. Proof has to be established on which party compromised card details.

b. Where a non EMV card is used on an EMV Terminal and fraud occurs, liability is on the Card Issuer

c. Where an EMV card is used on a non EMV Terminal and fraud occurs, liability is on the Acquirer

d. Where an EMV card is used on an EMV Terminal and fraud occurs, liability is on

the Card Holder or the Issuer. However, the onus is on the cardholder to

e. Where a hybrid card is used on an EMV Terminal and card treated as magnetic stripe for authorization and fraud occurs, liability is on the Card Issuer

f. Where a hybrid card is used on an EMV Terminal and card treated as EMV for authorization and fraud occurs, liability is on the Card Holder or the Issuer. However, the onus is on the cardholder to prove that his/her PIN had not been disclosed to a third party willingly or negligently.

1.8 Regulatory Monitoring

a. Any institution which operates an automated teller machine shall file an updated list of such ATMs, including the detail location of their addresses with Banking & Payments System Department of the Central Bank of Nigeria for compliance monitoring.

b. The CBN shall conduct onsite snap checking of ATMs with a view to ensuring compliance with cash and service availability at the ATMs.

c. Acquirers shall report volume and value of transactions on monthly basis to the Director, Banking & Payments System Department, CBN.

1.9 Penalties

Sanctions, in the form of monetary penalties / or suspension of the acquiring/processing service (s) or both, would be imposed on erring institutions for failure to comply with any of the provisions of the ATM standards and guidelines or any other relevant guidelines issued by the CBN from time to time.

2.0 GUIDELINES ON POINT OF SALE (POS) CARD ACCEPTANCE SERVICES

2.1 Objectives

These guidelines have been developed to provide minimum standards and requirements for the operation of POS card acceptance services under the following POS environment:

i. Countertop
ii. Wireless/Portable
iii. Handover (PIN Entry only/Customer-activated with PIN Entry)
iv. Automated Dispenser (e.g. Automated Fuel Dispenser, Token dispenser, etc)
v. Biometric point of sale
vi. Contactless

2.2 Point of Sale Card Acceptance Services Stakeholders

POS Card Acceptance Services Stakeholders include but not limited to:

i. Merchant Acquirers
ii. Card Issuers
iii.Merchants
iv. Cardholders
v. Card Schemes and Card Associations
vi. Switches
vii. Payments Terminal Service Aggregator (PTSA)
viii. Payments Terminal Service Providers (PTSP)

2.3 Minimum Standards

All industry stakeholders who process and/or store cardholder information shall ensure that their terminals, applications and processing systems comply with the minimum requirements of the following Standards and Best Practices (for PCI, the minimum requirement will be level 2.1). In addition, all terminals, applications and processing systems, should also comply with the standards specified by the various card schemes. Each vendor must provide valid certificates showing compliance with these standards, and must regularly review status of all its terminals to ensure they are still compliant as standards change. There will be a continuous review and recertification on compliance with these and other global industry standards from time to time.

2.3.1 PA DSS –Payment Application Data Security Standard.

2.3.2 PCI PED – Payment Card Industry Pin Entry Device.

2.3.3 PCI DSS – Payment Card Industry Data Security Standard.

2.3.4 Triple DES – Data Encryption Standards should be the benchmark for all data transmitted and authenticated between each party. The triple DES algorithm is the minimum standard.

2.3.5 EMV – The deployed infrastructure must comply with the minimum EMV requirements.

2.3.6 Each vendor must provide valid certificates showing compliance with these standards.

2.4 Roles and Responsibilities of:

2.4.1 Merchant Acquirers

2.4.1.1 Only CBN licensed institutions shall serve as Merchant Acquirers.

2.4.1.2 Merchant Acquirers can own POS Terminals, but shall only deploy and support POS terminals through a CBN licensed Payment Terminal Services Provider (PTSP). However, exceptions can be granted by the CBN where PTSP services are not available.

2.4.1.3 Merchant Acquirers shall ensure that POS terminals purchased and deployed at merchant/retailer locations through CBN licensed Payment Terminal Services Provider shall accept all cards (card agnostic).

2.4.1.4 Merchant Acquirers shall enter into agreements/contracts with merchants for accepting payment by means of electronic payment instrument. All agreements /contracts shall clearly spell out the terms and conditions, including roles, responsibilities and rights of the acquirer and the merchant. The contract should also clearly spell out requirements for the merchant's responsibilities in ensuring proper upkeep of the POS terminal.

2.4.1.5 Every Merchant Acquirer shall connect all its PoS terminals or other acquiring devices directly to any Payments Terminal Service Aggregator.

2.4.1.6 Merchant Acquirers shall switch all domestic transactions through the preferred

local switch of their choice for purpose of seeking authorization from the relevant Issuer.

2.4.1.7 To achieve interoperability, all POS terminals deployed in Nigeria shall accept all transactions arising from any card issued by any Nigerian bank. Accordingly, Acquirers and other service providers shall be card neutral entities that have no reason to promote or favour any card brand over the other.

2.4.1.8 Every acquirer must be able to accept all cards issued by Nigerian Banks, whether through a direct license or via an arrangement with any other acquirer that is licensed under the relevant card scheme/association.

2.4.1.9 Merchant Acquirers, in conjunction with their Payment Terminal Service Providers, shall be responsible for ensuring that merchants are trained and made to put in place reasonable processes and systems for confirming cardholder identity and detecting suspicious or unauthorized usage of electronic payment instruments where customer/card is physically present at point of sale.

2.4.1.10 Merchant Acquirers shall be required to undertake measures to prevent the use of their networks for purposes associated with money laundering and other financial crimes.

2.4.1.11 Merchant Acquirers shall conduct proper KYC on all their merchants with POS.

2.4.1.12 Merchant Acquirers shall set merchant limits based on the volume of business/type of commercial activities. In addition, Merchant Acquirers shall provide guidelines to merchants on payment procedures for large ticket transactions (e.g. review of Identification, etc.

2.4.1.13 Merchant Acquirers shall in conjunction with banks, switches and other stakeholders ensure resolution of disputed transactions between the merchant and the cardholder within five (5) working days. All transactions from POS devices shall be routed through the PTSA to the relevant acquirer or its appointed third party processor. Merchants shall provide evidence to dispute requests from the Acquirers within 48 hours failure of which their accounts shall be debited for the value of transaction.

2.4.1.14 There shall be no exclusivity arrangements that bundle third party switching

activities. Each acquirer shall be free to process transactions on its own, or leverage the services of a third party processor; and these services shall be independent of the switch used to facilitate such exchange.

2.4.1.15 Merchant Deposit Banks shall maintain and reconcile merchant accounts on behalf of the Merchant.

2.4.2 Payment Terminal Services Provider (PTSP)

2.4.2.1 To ensure effectiveness of POS operations and a proper support/maintenance infrastructure, only CBN licensed Payments Terminal Service Providers shall deploy, maintain and provide support for POS terminals in Nigeria. PTSPs shall offer services to acquirers covering all aspects relating to terminal management and support, including but not limited to purchase and replacement of spare parts, provision of connectivity, training, repairs, and development of value-added services, amongst other things.

2.4.2.2 CBN shall license a limited number of Payments Terminal Service Providers, to enable the PTSPs build scale and maximize efficiency. Criteria for PTSPs shall be defined by CBN, and the performance of licensed PTSPS shall be reviewed annually to confirm they meet defined performance targets. Licenses of PTSPs that fail to meet performance expectations can be withdrawn and fresh licenses issued to qualifying companies.

2.4.2.3 PTSPs can identify merchant opportunities and market potential merchants on behalf of acquirers.

2.4.2.4 Only PSTPs shall be allowed to deploy POS terminals. Any party, other than a PTSP that deploys POS terminals, shall be fined 50,000 Naira per day that terminal remains deployed. PTSPs shall clearly agree SLAs on deployment timelines with acquirers to ensure efficient deployment of POS terminals.

2.4.2.5 PSTPs shall ensure that deployed POS terminals are functional at all times. Appropriate mechanism must be put in place to remotely detect failures which shall be rectified or replaced within 48 hours.

2.4.2.6 All terminals deployed by PTSPs must have stickers with the PTSP's support service contact information. In addition PTSPs must have a support infrastructure that ensures support coverage for merchants 7 days a week.

2.4.2.7 PTSPs will be required to enter into contracts/SLAs with the acquirers that will clearly state the terms and conditions of their support services.

2.4.2.8 PTSPs shall work with the PTSA to ensure all POS terminals deployed by them meet all required certifications and the minimum POS specifications defined in these guidelines.

2.4.2.9 PTSPs shall work with acquirers and the terminal manufacturers to ensure that terminals are phased out/replaced/upgraded as appropriate, as their certifications become obsolete.

2.4.3 PoS Terminal Owner

2.4.3.1 Banks, Merchants, Acquirers, PTSA, and PTSPs can be PoS Terminal Owners.

2.4.3.2 PoS Terminal Owners shall ensure all POS terminals procured by them are compliant with the minimum POS specifications.

2.4.3.3 PoS Terminal Owners shall cover the costs of repairs and replacements of parts for their terminals.

2.4.4 Payments Terminal Service Aggregator (PTSA)

2.4.4.1 Nigeria Interbank settlement Systems (NIBSS) - owned by all Nigerian banks and the Central Bank of Nigeria shall act as the Payments Terminal Service Aggregator for the financial system.

2.4.4.2 As the Payments Terminal Service Aggregator for the industry, NIBSS shall establish communication network for reliable POS data traffic that shall satisfy the service and availability standards and expectations of the industry on a cost effective basis.

2.4.4.3 As the Payments Terminal Service Aggregator for the industry, NIBSS shall on an annual basis or more frequently as may be required, on behalf of the industry certify POS Terminals that meet the POS Terminal standards approved for the industry.

2.4.4.4 As the Payments Terminal Service Aggregator, NIBSS shall participate on a joint committee of industry stakeholders, to negotiate a price list with 2 – 3 terminal equipment providers for bulk purchase of POS terminals for the Nigerian market. It is expected that a bulk purchase agreement will enable cost reduction on POS terminals, as well as the ability to define special requirements for the Nigerian

market, and ensure a sufficient support infrastructure from the terminal manufacturers. Any Terminal Owner may subscribe to the negotiated global price list for the purchase of POS Terminals to take advantage of these benefits.

2.4.4.5 As the Payment Terminal Service Aggregator, NIBSS shall be the only entity permitted to operate a Terminal Management System. All POS terminals operating in Nigeria must be connected to the Payment Terminal Service Aggregator. This is to ensure comprehensive oversight, reporting/performance monitoring, and also in line with our objectives of shared industry infrastructure and best practice. NIBSS shall provide Acquirers and Payment Terminal Service Providers and their merchants (where required) the ability to view transactions and monitor performance of their devices.

2.4.4.6 All PoS Terminals deployed shall be technically enabled to accept all cards issued by Nigerian banks.

2.4.4.7 The Payments Terminal Service Aggregator (s) shall route all transactions from PoS terminals to the relevant Acquirer or its designated third party processor. This enables Acquirers who are Issuers to handle On-Us transactions appropriately and all Acquirers to manage their risks and accept responsibility for such transactions in line with Charge-back Rules of relevant Card Schemes. This does not preclude any Acquirer from using the services of any Third Party Processor (TPP) or the Acquirer's in-house processing services to process its acquired transactions.

2.4.4.8 All domestic transactions including but not limited to POS and ATM transactions in Nigeria must be switched using the services of a local switch and shall not under any circumstance be routed outside Nigeria for switching between Nigerian Issuers and Acquirers.

2.4.4.9 The Payments Terminal Service Aggregator(s) shall monitor the availability and transaction traffic on all POS terminals on a continuous basis and shall provide analysis and reporting on POS terminal performance and transaction trend to the Central Bank and the industry.

2.4.4.10 The Payments Terminal Service Aggregator (s) shall ensure all merchants and other relevant parties are settled within the T+1 settlement period, upon receipt of settlement reports from all card schemes or the switches they have appointed to provide such reports on their behalf. Failure to execute the T+1 settlement cycle shall result in a sanction to the PTSA, including but not limited to them solely

refunding the entire Merchant Service Charge for that day's transactions.

2.4.4.11 The Payments Terminal Service Aggregator shall have clear Service Level Agreements for certifying terminals quickly and efficiently, as well as for integrating new value-added services on behalf of acquirers, PTSPs, or 3rd party application developers.

2.4.5 Merchants

2.4.5.1 A merchant shall enter into agreement with Merchant Acquirer specifying in clear terms the obligations of each party.

2.4.5.2 Merchant shall accept cards as a method of payment for goods and services.

2.4.5.3 The merchant shall display the payment device conspicuously enough for the cardholder to observe the amount entered into the device before the cardholder enters his/her PIN.

2.4.5.4 The merchant shall be held liable for frauds with the card arising from its negligence, connivance etc.

2.4.5.5 A merchant shall under no circumstance charge a different price, surcharge a cardholder or otherwise discriminate against any member of the public who chooses to pay with a card or by other electronic means.

2.4.6 Cardholders

2.4.6.1 A cardholder shall:

a) Store the payment card and protect his PIN with due care
b) Not keep his payment card together with the PIN
c) Notify the issuer without delay about missing, stolen, damaged, lost or destroyed card
d) Not make available the payment card to unauthorized persons.

2.4.6.2 The cardholder may withdraw from the contract for payment card without prior notice to the issuer provided he does not owe for any charges or transactions on the payment card.

2.4.6.3 The cardholder shall present, when required by a merchant, a document confirming his identity.

2.4.6.4 The cardholder shall receive value for the operations performed by means of a payment card, and by so doing, the holder commits himself to pay the amount of the operations together with charges due to the issuer from a specified account.

2.4.6.5 The cardholder shall be held liable for fraud committed with his card arising from the misuse of his PIN or his card.

2.4.6.6 The cardholder shall be entitled to receive a receipt or any other form of evidence at the time a transaction is performed with his/her card

2.4.6.7 The cardholder shall be entitled to receive, within a reasonable period, at least monthly, a statement of all transactions performed with his/her card

2.4.6.8 If a cardholder notifies his bank that an error involving his card has occurred, the institution must investigate and resolve the claim within ~~3~~ 5 working days.

2.4.6.9 A cardholder shall be given reasonable notice before changes are made to the terms and conditions of his card contract and shall be given the option to opt-out of the card contract without penalty.

2.4.7 Card Associations and Card Schemes

2.4.7.1 All card associations and card schemes doing business in Nigeria are bound by these guidelines and other relevant CBN guidelines/circulars.

2.4.7.2 CBN shall reserve the right to assess the rules to confirm objectivity, vis-a-vis international standards/best practice. Any Card Scheme that wrongfully denies membership or unnecessarily delays the process of certification to potential players, would be penalized by CBN – including but not limited to paying a fine equivalent to the expected revenue of the payment services provider for that period, suspension and/or revocation of license, and CBN licensing new schemes.

2.4.7.3 No Card Scheme shall engage in the business of acquiring; neither shall any

entity that has a management contract with a Card scheme engage in the business of acquiring. In addition, no entity in which a Card Scheme, its subsidiary, or the majority shareholder of a card scheme, has 20% shareholding or more shall engage in the business of acquiring.

2.4.7.4 No Card Association or Card Scheme shall engage in any antitrust activity or any act that will lead to abuse of dominant position, monopoly or unfair competition. Accordingly, there shall not be any form of arrangement or collusion between two or more Card Associations, Card Schemes, or Payment Schemes in respect of Issuing, Acquiring, Processing or Switching.

2.4.8 Switching Companies

2.4.8.1 All local switches in Nigeria shall ensure that transactions relating to all cards issued by Nigerian banks are successfully switched between Acquirers and Issuers.

2.4.8.2 To achieve the interconnectivity of all new and existing switching companies, all switching companies shall open their networks for reciprocal exchange of transactions/messages with the Nigeria Central Switch and Payment Terminal Service Aggregator.

2.5 Settlement Mechanism

2.5.1 The settlement for all POS transactions must be done to the merchant account on T+1 basis, where T is the date the transaction is performed.

2.5.2 Card schemes or their appointed switches shall provide their settlement reports to NIBSS by 10am for the previous day. The settlement information should contain sufficient detail to enable NIBSS credit merchant accounts directly, and shall be provided in a format as advised by NIBSS. Failure to provide this information in the required format or by the required timeline will result in a sanction, including but not limited to the offending party solely refunding the entire Merchant Service Charge for that day's transactions.

2.5.3 NIBSS shall also directly credit the accounts of other parties with their share of the Interchange

2.5.4 NIBSS will be paid by the banks for the settlement done to the merchant account in

line with the NEFT fee transaction charges.

2.6 Fees and Charges

2.6.1 Fees and charges for POS Card Acceptance services are to be agreed between service providers and banks / entities to which the services are being provided subject to the following limits:

- The maximum total fee that a merchant shall be charged for any POS transaction shall be subject to negotiation between the acquirer and the merchant.
- The fees and charges stated above are applicable to only POS transactions performed with naira denominated cards. POS transactions done with cards issued in foreign currencies will still follow the pricing arrangement put in place by the relevant international card association/scheme.

2.7 Transition to Achieve Interoperability

All commercial switches, processors or entities driving PoS terminals in Nigeria shall ensure full and secure connection to the Central Switch and all transactions in respect of any card that the switch, processor or other entity is not licensed to process or switch shall be routed through the NCS to a licensed switch or processor for purpose of processing such transaction on behalf of the relevant Acquirer for seeking authorisation from the relevant Issuer.

All terminals must be plugged to the PTSA.

2.8 Exclusivity Agreements

There shall be no form of exclusivity in any area of payment service including but not limited to Issuing, Acquiring, Processing, and Sale and Maintenance of hardware and software. .Any payment scheme, operator, processor, infrastructure provider, switching company, service provider or bank that contravenes this policy may be suspended for a minimum of one (1) month by the CBN as a payment service or payment infrastructure service provider in the first instance, to be followed by stricter sanctions if the practice persists.

2.9 Minimum POS Terminal Specifications

Parameters	Specifications
Card Readers	EMV Chip/Smart cards, Magnetic stripe. Optional: Contactless reader, 2 SIM Slots
Communications	GPRS, Ethernet, Dial-up Modem. Optional: CDMA, Wi-Fi
Certifications	EMV levels 1 & 2, PCI DSS, PA-DSS, PCI PED online & offline (All PCI certifications should be Level/Version 2.1 minimum)
CPU	ARM9/11, 32Bits. Optional: Dual processors
Memory	16MB Flash, 32MB SDRAM
Keypad	PCI PED Approved, Backlit
Display	TFT LCD graphics, 128/64 pixel, Backlit. Optional: Colour screen
Power	100-240V, 50-60Hz; 24hrs battery power (operating) Optional: DC support, Car jack charger, Docking fast charger
Printer	15 -18 lines per sec Thermal printer
Multi-Application	Supports Multiple Applications
Customization / Others	Optional: Coloured or branded housing, Labelling/embossing, RS232 & USB interfaces, Protocol implementation

2.10 Compliance

All parties shall comply with the provisions of these guidelines and other relevant guidelines issued by the CBN. This guideline shall prevail in the case of conflict with any guidelines issued prior. Non compliance with the guidelines shall attract appropriate sanctions by CBN.

3.0 GUIDELINES ON MOBILE POINT OF SALE (mPOS) ACCEPTANCE SERVICES

3.1 Objectives

These Guidelines have been developed to:

3.1.1 Provide minimum standards and requirements for the operation of mPOS Acceptance Services that are not strictly dedicated to payment transaction processing, under the following environment:

i. Feature phones
ii. Smart phones
iii. Tablets
iv. Personal Digital Assistants (PDAs)
v. Contactless

3.1.2 Promote safety and effectiveness of mPOS and thereby enhance user confidence in the service.

3.1.3 Identify the roles and responsibilities of stakeholders

3.2 Minimum Standards

All industry stakeholders who process and/or store cardholder information shall ensure that their applications and processing systems comply with the following minimum requirements and standards:

3.2.1 All applications and processing systems shall comply with the standards specified by various card schemes. The minimum requirement for PCI shall be PCI DSS level 2.1.

3.2.2 Solution providers shall, in the case of dedicated mobile devices, be required to build Mobile POS solutions that utilize Payment Card Industry PIN Transaction Security (PCI PTS) in accordance with the PCI Point-to-Point Encryption (P2PE) Solution Requirements.

3.2.3 Each solution provider shall provide valid certificates showing compliance with the standards in 3.1 and 3.2; and shall regularly review the status of its applications to ensure they are in compliance with the following:

i. PA DSS –Payment Application Data Security Standard.

ii. PCI PED – Payment Card Industry Pin Entry Device.

iii. PCI DSS – Payment Card Industry Data Security Standard.

iv. Triple DES – Data Encryption Standards should be the benchmark for all data transmitted and authenticated between each party.

v. EMV – The deployed infrastructure must comply with the minimum EMV requirements.

3.2.4 Merchants shall be required to use Mobile POS solutions that utilize P2PE solutions in accordance with the *PCI Point-to-Point Encryption Solution Requirements*.

3.3 Mobile Point of Sale (mPOS) Stakeholders

The parties involved in payments acceptance and processing for mPOS shall include:

i. Acquirer

ii. Issuer

iii. PTSA

iv. Merchant

v. Cardholder/User

vi. Card Associations and Card Schemes

vii. Switches

viii. PSSP

3.4 Roles and Responsibilities of:

3.4.1 Acquirers

3.4.1.1 Only CBN licensed institutions shall serve as Acquirers.

3.4.1.2 Either Acquirer or Merchant may own an mPOS device however; a Dedicated Device shall only be deployed by an Acquirer.

3.4.1.3 Acquirers shall ensure that mPOS devices purchased and deployed at merchant/retailer locations accept all cards (card agnostic).

3.4.1.4 Acquirers shall enter into agreements/contracts with merchants for the acceptance of payments by means of electronic payment instrument. All agreements/contracts shall clearly spell out the terms and conditions, including roles, responsibilities and rights of the Acquirer and the merchant.

3.4.1.5 Every Acquirer shall connect all its mPOS devices directly to any Payments Terminal Service Aggregator.

3.4.1.6 The Acquirers shall switch all domestic transactions through the preferred local switch of their choice for purpose of seeking authorisation from the relevant Issuer.

3.4.1.7 The Acquirers shall be required to undertake measures to prevent the use of their networks for purposes associated with money laundering and other financial crimes and shall conduct proper KYC on all their merchants.

3.4.1.8 The Acquirers shall set merchant limits based on the volume of business/type of commercial activities. In addition, Acquirers shall provide guidelines to merchants on payment procedures for large ticket transactions (e.g. review of Identification, etc)

3.4.1.9 There shall be no exclusivity arrangements that bundle third party processing with switching activities. Each Acquirer shall be free to process transactions on its own, or leverage the services of a third party processor; and these services shall be independent of the switch used to facilitate such exchange.

3.4.1.10 The Acquirers shall maintain and reconcile merchant accounts.

3.4.1.11 The Acquirer shall provide the merchant with a PTSA certified card reader and the mPOS application for the handheld device; and where the card reader is in-built, the Acquirer shall ensure that the device is certified by the PTSA.

3.4.1.12 The Acquirer shall ensure that the mPOS application is PA-DSS certified.

3.4.1.13 The Acquirer shall assess and determine the suitability of mPOS for a merchant with consideration for the merchant's control environment and other additional responsibilities for using mPOS.

3.4.1.14 An Acquirer shall not acquire transaction through mPOS for a merchant it assesses as having a weak control environment, for managing mPOS devices.

3.4.1.15 The Acquirer shall ensure an effective patch and version control management for the mobile application on the merchant's mPOS devices.

3.4.1.16 The Acquirer shall ensure that it does not acquire transactions from an mPOS device whose payments processing application is not updated with most recent patches, anti-virus and upgrades.

3.4.1.17 The Acquirer shall ensure the implementation of an enterprise mobility management system for the mPOS devices of the merchants it is acquiring.

3.4.1.18 The Acquirer shall ensure that payments data are transmitted using secured communication channels and protocols with end-to-end encryption as specified in POS guidelines.

3.4.1.19 The Acquirer shall be responsible for the back-end payment processing. The back-end payments processing and settlement shall comply with extant POS guidelines.

3.4.1.20 The Acquirer shall be responsible for sensitizing/educating the merchant on security measures required for the mPOS device.

3.4.1.21 The Acquirer shall ensure that the mPOS is capable of issuing receipts either in electronic or paper form upon consummation of a transaction.

3.4.1.22 The Acquirer and the merchant shall be responsible for the maintenance of the card reader.

3.4.1.23 The Acquirer shall ensure that card readers are configured as merchant-specific.

3.4.1.24 The Acquirer shall ensure that mPOS applications are lockdown such that other mobile applications on the mPOS devices of the merchants do not interact, store or transmit payment data.

3.4.2 Issuers

The responsibilities of Issuers shall be as stipulated in the extant POS Guidelines.

3.4.3 Payments Terminal Service Aggregator (PTSA)

3.4.3.1 Nigeria Interbank Settlement Systems (NIBSS) shall act as the Payments Terminal Service Aggregator for the financial system.

3.4.3.2 As the Payments Terminal Service Aggregator for the industry, NIBSS shall establish communication network for reliable data traffic that shall satisfy the service and availability standards and expectations of the industry on a cost effective basis.

3.4.3.3 As the Payments Terminal Service Aggregator for the industry, NIBSS shall on an annual basis or more frequently as may be required, certify mPOS devices that meet the industry standards.

3.4.3.4 As the Payment Terminal Service Aggregator, NIBSS shall be the only entity permitted to operate a Terminal Management System.

3.4.3.5 The Payments Terminal Service Aggregator (s) shall route all transactions from mPOS devices to the relevant Acquirer or its designated third party processor. This enables Acquirers who are Issuers to handle On-Us transactions appropriately and all Acquirers to manage their risks and accept responsibility for such transactions in line with Charge- back Rules of relevant Card Schemes. This does not preclude any Acquirer from using the services of any Third Party Processor (TPP) or the Acquirer's in-house processing services to process its acquired transactions.

3.4.3.6 All mPOS transactions in Nigeria must be switched using the services of a local switch and shall not under any circumstance be routed outside Nigeria for switching between Nigerian

3.4.4 Issuers and Acquirers.

3.4.4.1 The Payments Terminal Service Aggregator(s) shall monitor the availability and transaction traffic on all mPOS devices on a continuous basis and shall provide analysis and report on performance and transaction trend to the Central Bank of Nigeria.

3.4.4.2 The Payments Terminal Service Aggregator shall have clear Service Level Agreements for

certifying devices quickly and efficiently, as well as for integrating new value-added services on behalf of Acquirers and third party application developers.

3.4.5 Merchants

3.4.5.1 A merchant shall enter into agreement with the Acquirer specifying in clear terms the obligations of each party.

3.4.5.2 Merchant shall accept cards as a method of payment for goods and services.

3.4.5.3 The merchant shall display the payment device conspicuously for the cardholder/user to observe the amount entered into the device before the cardholder/user enters his/her PIN.

3.4.5.4 The merchant shall be held liable for frauds involving the use of mPOS device due to its negligence, connivance etc.

3.4.5.5 The merchant shall under no circumstance charge a different price, surcharge a cardholder/user or otherwise discriminate against any member of the public who chooses to pay with a card or by other acceptable electronic means.

3.4.5.6 The merchant shall ensure that it complies with the minimum security guidance provided by the Acquirer.

3.4.5.7 The merchant shall determine the location and condition of the mPOS device at all times and shall inform the Acquirer immediately it is unable to do so.

3.4.5.8 The Merchant shall be responsible for determining and maintaining inventory of other applications that co-exist on mPOS devices.

3.4.5.9 The merchant and the Acquirer shall be responsible for the maintenance of the mPOS device.

3.4.5.10 Merchant shall be responsible for restricting physical and logical access to the mPOS device.

3.4.6 Cardholders/Users

3.4.6.1 A cardholder/user shall:

i. Protect the payment card, mobile device and PIN with due care.
ii. Notify the issuer immediately a PIN is compromised.
iii. Notify the issuer without delay about missing, stolen, damaged, lost or destroyed card and/or mobile device.

3.4.6.2 The cardholder may withdraw from the contract for payment card without prior notice to the issuer provided he does not owe any charges for transactions on the payment card.

3.4.6.3 The cardholder shall present, when required by a merchant, a document confirming his identity.

3.4.6.4 The cardholder shall receive value for the operations performed by means of a payment card, and by so doing, the holder commits himself to pay the amount of the operations together with charges due.

3.4.6.5 The cardholder shall be held liable for fraud committed with his card arising from the misuse of his PIN or his card.

3.4.6.6 The cardholder/user shall be entitled to receive a receipt or any other form of evidence at the time a transaction is performed with his/her card.

3.4.6.7 The cardholder/user shall be entitled to receive, within a reasonable period, at least monthly, a statement of all transactions performed with his/her card.

3.4.6.8 If a cardholder/user notifies his bank of a transaction error, the issuer shall investigate and resolve the claim within 5 working days.

3.4.6.9 A cardholder/user shall be given not less than 5 working days notice before changes are made to the terms and conditions of his card contract and shall be given the option to opt-out of the card contract without penalty.

3.4.7 Card Associations and Card Schemes

All card associations and card schemes doing business in Nigeria are bound by these guidelines and other relevant CBN guidelines/circulars.

3.4.7.1 Any Card Scheme that wrongfully denies membership or delays the process of certification to potential players, would be penalized by CBN – including but not limited to paying a fine equivalent to the expected revenue of the payment services provider for that period, suspension and/or revocation of license, and shall not be eligible for further participation in CBN licensing schemes.

3.4.7.2 No Card Scheme, or any entity that has a management contract with a Card Scheme, shall engage in the business of acquiring. In addition, no entity in which a Card Scheme, its subsidiary, or the majority shareholder of a card scheme, has 20% shareholding or more shall engage in the business of acquiring.

3.4.7.3 No Card Association or Card Scheme shall engage in any antitrust activity or any act that will lead to abuse of dominant position, monopoly or unfair competition. Accordingly, there shall not be any form of arrangement or collusion between two or more Card Associations, Card Schemes, or Payment Schemes in respect of issuing, acquiring, processing or switching.

3.4.8 Switches (Switching Companies)

3.4.8.1 All local switches in Nigeria shall ensure that transactions relating to all cards issued by Nigerian banks are successfully switched between Acquirers and Issuers.

3.4.8.2 To achieve the interconnectivity of all new and existing switching companies, all switching companies shall open their networks for reciprocal exchange of transactions/messages with the Nigeria Central Switch and Payment Terminal Service Aggregator.

3.4.9 Payments Solution Service Providers (PSSPs)

Payment Solution Service Providers shall:

3.4.9.1 Be licensed by the Bank to provide end-to-end electronic payment solutions, systems and services to all stakeholders covered by these guidelines.

3.4.9.2. Publish customer service contact details and maintain customer service desks to promptly attend to all electronic payment enquiries and complaints within stipulated timelines.

3.4.9.3 Maintain, and make available to CBN, report of all electronic payment transactions

processed on their platform and report of customer complaints, indicating resolution status.

3.4.9.4 Comply with timelines for Returns as stipulated by CBN.

3.5 Settlement Mechanism

3.5.1 The settlement for all mPOS transactions shall be done to the merchant account on T + 1 basis, where T is the date the transaction is performed. Failure to execute the T+1 settlement cycle shall result in a sanction to the NIBSS.

3.5.2 Card schemes or their appointed switches shall provide settlement reports to NIBSS b10am for the previous day's transactions. The settlement information shall contain sufficient details in the required format as advised by NIBSS to enable direct credit into merchant accounts. Failure to provide this information within the timeline and in the prescribed format will result in a sanction.

3.5.3 NIBSS shall also directly credit the accounts of other parties with their share of the Interchange.

3.5.4 NIBSS will be paid by the banks for the settlement done to the merchant account in line with the NIBSS Electronic Funds Transfer (NEFT) fee transaction charges.

3.6 Fees and Charges

3.6.1 Fees and charges for mPOS Card Acceptance services are to be agreed between service providers and banks/entities to which the services are being provided subject to the following limits:

i. The maximum total fee that a merchant shall be charged for any mPOS transaction shall be subject to negotiation between the Acquirer and the merchant.

ii. The fees and charges stated above are applicable to only mPOS transactions performed with naira denominated cards. mPOS transactions done with cards issued in foreign currencies will still follow the pricing arrangement put in place by the relevant international card association/scheme.

3.7 Transition to Achieve Interoperability

All commercial switches, processors or entities driving mPOS devices in Nigeria shall ensure full and secure connection to the Central Switch and all transactions in respect of any card that the switch, processor or other entity is not licensed to process or switch shall be routed through the NCS to a licensed switch or processor for purpose of processing such transaction on behalf of the relevant Acquirer for seeking authorisation from the relevant Issuer.

All mPOS devices must be plugged to the PTSA.

3.8 Exclusivity Agreements

There shall be no form of exclusivity in any area of payment service including but not limited to issuing, acquiring, processing, and sale and maintenance of hardware and software. Any payment scheme, operator, processor, infrastructure provider, switching company, service provider or bank that contravenes this policy may be suspended for a minimum of one (1) month by the CBN in the first instance, to be followed by stricter sanctions if the practice persists.

3.9 Minimum mPOS Technical Specifications

Parameters	Specifications
Card Readers	EMV Chip/Smart cards, Magnetic stripe, supporting audio jack interface and/or Bluetooth communications interface. Optional: Contactless reader.
Communications	GPRS, Ethernet, Dial-up Modem. Optional: CDMA, Wi-Fi
Certifications	EMV levels 1 & 2, PCI DSS, PA-DSS, PCI PED online & offline (All PCI certifications should be Level/Version 2.1 minimum)
CPU	ARM9/11, 32Bits. Optional: Dual processors
Memory	16MB Flash, 32MB SDRAM
Keypad	PCI PED Approved, Backlit
Display	TFT LCD graphics, 128/64 pixel, Backlit. Optional: Colour screen
Power	100-240V, 50-60Hz; 24hrs battery power (operating) Optional: DC support, Car jack charger, Docking fast charger
Printer	15 -18 lines per sec Thermal printer
Multi-Application	Supports Multiple Applications
Customization / Others	Optional: Coloured or branded housing, Labelling/embossing, RS232 & USB interfaces, Protocol implementation

3.10 Consumer Protection/Dispute Resolution

3.10.1 Acquirers shall in conjunction with issuers, switches and other stakeholders ensure resolution of disputed transactions between the merchant and the cardholder within five (5) working days.

3.10.2 Merchants shall provide evidence of dispute requests to the Acquirers within 48 hours, failing which their accounts shall be debited for the value of transaction.

3.10.3 Stakeholders/Parties may escalate complaints to the CBN where they are dissatisfied with 11.1 and 11.2 above.

3.10.4 Any dispute, controversy or claim arising out of or relating to this Guidelines or the breach, termination or invalidity thereof shall be settled in accordance with the CBN's dispute resolution mechanism and if unresolved may refer to an arbitral panel as provided under the Arbitration and Conciliation Act Cap. A18 LFN 2004.

3.11 Compliance

All parties shall comply with the provisions of these Guidelines and other related guidelines issued by the CBN. Noncompliance with the guidelines shall attract appropriate sanctions by CBN.

These Guidelines shall prevail in the case of conflict with any prior guidelines issued by the CBN.

4.0 GUIDELINES ON WEB ACCEPTANCE SERVICES

4.1 Scope of the Guidelines

These Guidelines shall include all forms of transfer of monetary value on the website of a merchant or a payment aggregator in fulfillment of consideration for the purchase of goods and services on the internet by means of:

- Cards payments
- Credit transfers
- Direct debit electronic mandates
- Electronic Wallet/Virtual card/Electronic money.

4.2 Objectives

These Guidelines shall:

4.2.1 Provide minimum standards and requirements for the processing of card transactions via the web (internet) channel.

4.2.2 Promote safety and effectiveness of Web Acceptance Services and thereby enhance user confidence in the service.

4.2.3 Identify the roles and responsibilities of stakeholders

4.2.4 Encourage the development of effective, low risk, low cost and convenient payment and financial services to customers and businesses through the internet

4.3 Minimum Standards

All industry stakeholders who process and/or store cardholder information shall comply with the following standards:

i) PCI DSS- Payment Card Industry Data security standard

ii) PA DSS- Payment Application Data Security Standard

iii) Triple DES- Data Encryption Standards should be the benchmark for all data transmitted and authenticated between each party.

iv) EMV- The deployed infrastructure must comply with the minimum EMV requirements.

4.4 Licensing of Web Acceptance Services

For a company to operate web acceptance services in Nigeria, it shall obtain an approval from the CBN.

4.5 Stakeholders

The following parties in a web payment scenario have responsibilities for web payments transactions

i. Acquirer: including a CBN licensed web payment aggregator
ii. Issuer
iii. Merchant (website owner)
iv. Payments Gateway Providers
v. Payments Solution Service Providers
vi. cardholder

4.6 Roles and Responsibilities of Stakeholders

4.6.1 Acquirer

In addition to the basic responsibilities of an acquirer as stipulated in extant guidelines, with respect to web payments, the acquirer shall:

4.6.1.1 Only CBN licensed financial and non-financial institutions shall serve as acquirers to merchants that accept card transactions on their website.

4.6.1.2 Be responsible for engaging and managing the payments integrator (gateway).

4.6.1.3 Evaluate the merchant web application, technology and control environment and ensure that it is implemented securely to accept payments.

4.6.1.4 Carry out appropriate regular threat scan on the merchant's website and avail the merchant with updates on emerging threats to ensure that appropriate measures are taken by the merchant to mitigate risks.

4.6.1.5 Test website payment integration and ensure that sensitive customer data are not retained on the merchant's website.

4.6.1.6 For the minimum Web Capabilities of ecommerce websites/web portal**,** Acquirers and service providers shall comply with scheme rules as defined by the various card schemes, however, where there is conflict this Guidelines supersedes.

4.6.1.7 The acquiring bank can also be a merchant and deploy/implement a website to accept card payments for its own services or services provided by merchants acquired by them.

4.6.1.8 The Acquiring Bank shall assist the Merchant in setting up the accounts in the bank and any back-end processing for settlement of payments done on the merchant website using cards.

4.6.1.9 The Acquiring Bank shall acquire all transactions done on the website of Merchants acquired by them.

4.6.1.10 The acquiring bank shall sign an agreement with the merchant for accepting card payment via the web channel.

4.6.1.11 The acquiring bank shall perform adequate Customer Due Diligence (CDD), Know-your-Customer (KYC) and Know-your-Customer-Business KYC/B on the merchant.

4.6.1.12 The acquiring bank shall maintain and reconcile merchant accounts on behalf of the merchant.

4.6.1.13 The Acquiring Bank reserves the right to discontinue acquiring for a merchant at any time for proven cases of fraud, consistent failed deliveries and other situations involving the Merchant, which may impact negatively on the industry.

4.6.1.14 Acquirers shall implement a fraud management system that will detect customer usage pattern and decline/accept transaction based on rules defined on the fraud management system.

4.6.1.15 Acquirers shall categorize merchants based on the services being offered and define transaction limits in conjunction with the issuer.

4.6.2 Merchants

The merchant, in addition to the basic responsibilities as stipulated in extant guidelines, shall:

4.6.2.1 Ensure that the terms and conditions for its products and services are properly communicated and conspicuously displayed on its website.

4.6.2.2 Ensure that it cooperates with the Acquirer in implementing appropriate security measures.

4.6.2.3 Provide the customer with clear instructions on the process for making payments on its websites.

4.6.2.4 Provide information to customers on the charges applicable to each web payment option on its website.

4.6.3 Issuer

The issuer, in addition to its responsibilities under the various extant guidelines (POS and Card Issuance), shall:

4.6.3.1 Be responsible for the issuance of the cards. Only licensed deposit taking banks shall serve as the issuers of payment cards.

4.6.3.2 In the event of a dispute, provide information / reports on the transaction, and aid in the prompt resolution of issues within 72 hours of date it was reported.

4.6.3.3 Issue only EMV compliant cards.

4.6.3.4 Commit to authorize the cardholder transaction made from the card linked to a specified account in the issuing bank and settle the operations performed by the means of the card.

4.6.3.5 Provide additional security measures e.g. second factor authentication to cardholders who intend to utilize their cards for transactions via the web channel.

4.6.3.6 Be held liable for card fraud in the event that payments are made with hot listed cards or where a card is reported as lost or stolen and subsequently used to make payments on any other channel.

4.6.3.7 Provide means through which cardholders can, at any time, notify the issuer of any loss, theft or fraudulent use of the card and the issuer shall take all necessary steps to stop any further use of the card.

4.6.3.8 Maintain internal records over a minimum period of seven (7) years to enable audit trails on card-related transactions.

4.6.3.9 Be responsible for setting overall transaction limits on cards per day, and transaction limits of such cards by channel, according to their card products and risk guidelines.

4.6.3.10 Respond to Card related disputes or complaints from cardholders within 24hours, and in conjunction with the Acquirer and platform provider resolve such disputes or complaints within 72 hours.

4.6.3.11 Furnish its cardholders with a detailed list of contractual terms and conditions prior to activation. Such terms shall include at a minimum, fees and charges, withdrawal limits (including offline transaction limits and terms where applicable), billing cycles, termination procedures, default/recovery procedures and loss/theft/misuse of card procedures.

4.6.3.12 Implement authentication at the "highly secured level" requiring in addition to static PIN/Password, one of the following :

i. One Time PIN/Password

ii. 3D Secure code

iii. Token code

4.6.3.13 Implement behavioral monitoring and SMS/email alerts as additional controls to further protect the payer.

4.6.4 Payments Gateway Provider

Payment Gateway Provider Shall:

4.6.4.1 Provide services with respect to the processing of online payment transactions related to the sale of goods and/or services.

4.6.4.2 Act as facilitator on behalf of cardholder/users:

i. to enable Payment Transactions; and
ii. processing authorisation requests.

4.6.4.3 Be responsible for the security of the data related to the payment instrument that is possessed or otherwise stored, processed or transmitted on behalf of cardholders/users.

4.6.4.4 Not store card details on any server maintained by either you or any third party without first undergoing a security audit carried out by a Qualified Security Assessor (QSA).

4.6.4.5 Hold all forms of customer data securely and take responsibility for the security of the data.

4.6.5 Payments Solution Service Provider

Payment Solution Service Providers shall:

4.6.5.1 Be licensed by the Bank to provide end-to-end electronic payment solutions, systems and services to all stakeholders covered by these guidelines.

4.6.5.2 Publish customer service contact details and maintain customer service desks to promptly attend to all electronic payment enquiries and complaints within stipulated timelines.

4.6.5.3 Maintain, and make available to CBN, report of all electronic payment transactions processed on their platform and report of customer complaints, indicating resolution status.

4.6.5.4 Comply with timelines for Transaction Completion and Unapplied Funds Returns as stipulated by CBN.

4.6.6 Cardholder

The cardholder shall:

4.6.6.1 Inform or request from the issuing bank that his/her card be enabled on the web channel.

4.6.6.2 Provide his card number, expiry date, PIN, CVV2 and One Time Password (OTP) when completing payments online.

4.6.6.3 Guard his card, PIN and hardware token with utmost care.

4.6.6.4 Immediately notify the issuer if the card, PIN or token is lost/compromised.

4.7 Settlement Mechanism

4.7.1 The settlement for all WEB transactions shall be made to the merchant account on a T+1 basis where T is the date the transaction is performed.

4.7.2 The Acquirer shall settle the funds to merchant account.

4.8 Fees

4.14.1 Fees shall be based on CBN Interchange Guidelines.

4.14.2 The interchange will be regulated by the Central Bank

4.14.3 An interchange fee is to be charged and will be between the acquirer and the issuer.

4.14.4 Other service providers will be free to negotiate their fees with the party that service is been rendered too

4.14.5 Web transactions done with cards issued in foreign currencies will follow the pricing arrangement put in place by the relevant international card association/scheme

4.9 Consumer Protection/Dispute Resolution

Any dispute, controversy or claim arising out of or relating to this Guidelines or the breach, termination or invalidity thereof shall be settled in accordance with the CBN's dispute resolution mechanism and if unresolved may refer to an arbitral panel as provided under the Arbitration and Conciliation Act Cap. A18 LFN 2004.

4.10 Compliance

All parties shall comply with the provisions of these guidelines and other related guidelines issued by the CBN. Noncompliance with the guidelines shall attract appropriate sanctions by CBN.

These guidelines shall prevail in the case of conflict with any prior guidelines issued by the CBN.

5.0 Definition of Terms

The terms below shall have the following meaning for the purpose of the Guidelines.

1) Issuer: Financial institution that issues plastic cards to customers

2) Acquirer means bank or any other legal person concluding contracts with merchants concerning acceptance of payment by means of electronic payment instrument.

3) Cardholder means any person who holds a payment card for the purpose of effecting payment in respect of goods and services.

4) Settlement Agent: Institution that generates financial data and compute net settlement position for each financial institution in a payment scheme(s).

5) PIN means Personal Identification Number

6) Payment tokens: Any authorized payment instruments (physical or electronic) used to initiate a transaction.

7) Switch means a system that captures electronic financial transactions from touch-points, applies rules, determines destinations, delivers the transactions and gives appropriate feedback;

8) EMV (Europay, MasterCard, Visa) is the global standard that is helping ensure smart (Chip-and-PIN) cards, terminals and other systems can interoperate.

9) PCI DSS stands for Payment Card Industry Data Security Standard. It was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud and various other security vulnerabilities and threats

10) Merchant Acquirer means a CBN licensed financial or non-financial institution that has agreement with the relevant card scheme to contract with merchants to accept payment cards as means of payment for goods and services.

11) Cardholder means any person to whom a payment card is issued and whose account will eventually be debited for settlement of transactions performed with the payment card.

12) Deposit Taking Banks means banks and other financial institutions.

13) Merchant means an organization or entity that contracts with a Merchant Acquirer for accepting payment by means of payment card or any other electronic payment instrument.

14) Operations include facilitation of funds transfer, effecting payment and such other transactions that may be determined from time to time by means of an electronic payment instrument.

15) Interoperability means ability to issue cards and deploy devices in such a way that all customers (card holders, merchants and issuers) perceive operations, while obtaining service, as if the interconnected networks were one.

16) Interconnectivity means ability for reciprocal exchange of transactions/messages between two or more switching networks.

17) PIN means Personal Identification Number.

18) Competent Authorities include Courts, Economic and Financial Crime Commission (EFCC), Independent Corrupt Practices Commission (ICPC), Regulatory Authorities such as the CBN, Nigeria Deposit Insurance Commission (NDIC) etc.

19) Hot list means list of deactivated cards that were reported missing, stolen, lost or damaged by the card holders.

20) Switch means a system that switches card payments messages between acquirer (or acquirer processor) and issuer (or issuer processor)

21) Card Schemes define the rules of the card system (e.g. interchanges, licenses, fraud responsibilities), and choices of technical functionalities (e.g. standards, protocols, security requirements)

22) Processor processes card transactions.

23) A Card Association is a network of issuing banks and acquiring banks that process payment cards of a specific brand.

24) EMV (Europay, MasterCard, Visa) is the global standard that is helping ensure smart (Chip-and-PIN) cards, terminals and other systems can interoperate.

25) PCI DSS stands for Payment Card Industry Data Security Standard. It was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud and various other security vulnerabilities and threats.

26) PCI PED stands for Payment Card Industry Pin Entry Device. PCI PED security requirements are designed to secure personal identification number (PIN)-based transactions globally and apply to devices that accept PIN entry for all PIN based transactions.

27) PA-DSS stands for Payment Application Data Security Standard. PA-DSS compliant applications help merchants and agents mitigate compromises, prevent storage of sensitive cardholder data, and support overall compliance with the PCI DSS.

28) NIBSS stands for Nigeria Inter-Bank Settlement System, it was mandated as act as the Automated Clearing House (ACH) for Nigeria.

29) mPOS stands for mobile Point of Sale. A smart phone, tablet or dedicated wireless device that performs the functions of an electronic Point of Sale (PoS) terminal.

30) Card Reader is an apparatus that reads data from a payment card. It may have an audio jack that is attachable to a port or may connect via Bluetooth to the mobile device.

31) mPOS Device for the purpose of this Guidelines, constitutes three components; the card reader, downloaded mobile app and the mobile phone or tablet that together, perform the functions of an electronic Point of Sale (PoS) terminal.

32) Dedicated mPOS is an mPOS device that is solely restricted to its primary function of facilitation of payments transactions.

33) Not-Dedicated-mPOS is an mPOS device that is used for facilitation of payments

transactions and other functions, including but not limited to making phone calls, internet surfing, games, GPRS etc

34) Feature phone is a phone that is although not a smart phone, but has additional functions over and above a standard phone.

35) Smart phone is a phone built on advanced mobile computing platform with superior capabilities than a feature phone.

36) Tablet is a mobile computer that is larger than a typical smart phone, with integrated features such as touch screen and is typically operated not by keyboard but through touching screen.

37) Near Field Communication (NFC) is the set of protocols that enables devices to establish radio communication with each other by touching each other or bringing them into proximity of a distance typically 10 cm (3.9 in) or less.

38) Contactless refers to a process of performing a transaction via NFC antenna embedded within the mobile device.

39) Acquirer means a CBN licensed financial or non-financial institution that has agreement with the relevant card scheme to contract with merchants to accept payment cards as means of payment for goods and services.

40) Cardholder means any person to whom a payment card is issued and whose account will eventually be debited for settlement of transactions performed with the payment card.

41) Deposit Taking Banks means banks and other financial institutions.

42) Merchant means an organization or entity that contracts with a Merchant Acquirer for accepting payment by means of payment card or any other electronic payment instrument.

43) Operations include facilitation of funds transfer, effecting payment and such other

transactions that may be determined from time to time by means of an electronic payment instrument.

44) Interoperability means ability to issue cards and deploy devices in such a way that all customers (card holders, merchants and issuers) perceive operations, while obtaining service, as if the interconnected networks were one.

45) Interconnectivity means ability for reciprocal exchange of transactions/messages between two or more switching networks.

46) PIN means Personal Identification Number.

47) Competent Authorities include Courts, Economic and Financial Crime Commission (EFCC), Independent Corrupt Practices Commission (ICPC), Regulatory Authorities such as the CBN, Nigeria Deposit Insurance Commission (NDIC) etc.

48) Hot list means list of deactivated cards that were reported by the card holders as missing, stolen, lost, compromised or damaged.

49) Switch means a system that switches card payments messages between Acquirer (or Acquirer processor) and issuer (or issuer processor)

50) Card Schemes define the rules of the card system (e.g. interchanges, licenses, fraud responsibilities), and choices of technical functionalities (e.g. standards, protocols, security requirements)

51) Processor processes card transactions.

52) A Card Association is a network of issuing banks and acquiring banks that process payment cards of a specific brand.

53) EMV (Europay, MasterCard, Visa) is the global standard that is helping ensure smart (Chip-and-PIN) cards, terminals and other systems can interoperate.

54) PCI DSS stands for Payment Card Industry Data Security Standard. It was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud and various other security vulnerabilities and threats.

55) PCI PTS stands for Payment Card Industry PIN Transaction Security requirements

are used primarily by ATM and point-of-sale device manufacturers to secure cardholder's details at physical point of entry.

56) PCI PED stands for Payment Card Industry Pin Entry Device. PCI PED security requirements are designed to secure personal identification number (PIN)-based transactions globally and apply to devices that accept PIN entry for all PIN based transactions.

57) PA-DSS stands for Payment Application Data Security Standard. PA-DSS compliant applications help merchants and agents mitigate compromises, prevent storage of sensitive cardholder data, and support overall compliance with the PCI DSS.

58) NIBSS stands for Nigeria Inter-Bank Settlement System, it was mandated to act as the Automated Clearing House (ACH) for Nigeria.

59) Point-to-Point Encryption (P2PE) is a method of protocol for data encryption ensuring secure transmission between two points.

60) Web is an information space where documents and other web resources are identified by uniform resource identifiers, interlinked by hypertext links, and accessible via the Internet.

61) Web Acceptance is the process of accepting payments through the web channel.

62) Acquirer means bank or any other legal person concluding contracts with merchants concerning acceptance of payment by means of electronic payment instrument.

63) Cardholder means any person who holds a payment card for the purpose of effecting payment in respect of good services.

64) Competent Authorities include Courts, EFCC, ICPC, Regulatory Authorities such as the CBN, NDIC etc

65) Hot list means list of deactivated cards that were reported missing, stolen, lost or damaged by the card holders.

66) Interconnectivity means ability for reciprocal exchange of transactions/messages between two or more switching networks.

67) Interoperability means ability to issue cards and deploy devices in such a way that all customers (card holders, merchants and issuers) perceive operations, while obtaining service, as if the interconnected networks were one.

68) Member Institutions means banks and other financial institutions that are on the network of a particular switching company;

69) Merchant means an organization or entity that undertakes to conclude a contract with an acquirer and / or issuer concerning accepting payment by means of an electronic payment instrument;

70) MPR means Minimum Policy Rate

71) Offline transaction means a transaction in which no direct connection is made between the device(s) involved in the transaction and a centralized computer system for the purpose of effecting settlement, or authenticating the transaction before it is executed.

72) Online transaction means a transaction in which there is a direct connection between the device(s) and a centralized computer system for effecting settlement or authorization or validation before a transaction can be executed.

73) Operations include facilitation of cash withdrawal, funds transfer, effecting payment and such other transactions that may be determined from time to time by means of an electronic payment instrument.;

74) PIN means Personal Identification Number

75) Switch means a system that captures electronic financial transactions from touch-points, applies rules, determines destinations, delivers the transactions and gives appropriate feedback;

76) EMV (Europay, MasterCard, Visa) is the global standard that is helping ensure smart (Chip-and-PIN) cards, terminals and other systems can interoperate.

77) PCI DSS stands for Payment Card Industry Data Security Standard. It was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud and various other security vulnerabilities and threats

78) PCI PED security requirements are designed to secure personal identification number (PIN)-based transactions globally and apply to devices that accept PIN entry for all PIN based transactions

79) Payments GP Payment Gateway is an e-commerce application service provider that authorizes card payments for e-businesses, online retailers, etc.

CENTRAL BANK OF NIGERIA

SEPTEMBER, 2015.