GUIDELINES ON TRANSACTIONS SWITCHING SERVICES

GUIDELINES ON TRANSACTIONS SWITCHING SERVICES

1.1 In exercise of the powers conferred on the Bank by Section 28 (1) (b) of the Central Bank of Nigeria Act 10991 (as amended) to issue guidelines for the maintenance of adequate and reasonable financial services for the public and to ensure high standards of conduct and management throughout the banking system; and

Pursuant to its inherent powers, the Central Bank of Nigeria (CBN) hereby issues the following guidelines for the operations of the switching services in Nigeria:

1.2 Scope of the Guidelines

The guidelines set out the procedures for the operation of switching services in Nigeria, including the rights and obligations of the parties to the switching contract. It also compels the switching companies to meet with minimum standards for switching as approved by the CBN.

1.3 License of Switching Companies

For a switching company to operate in Nigeria, it shall obtain a license from the CBN.

1.3.1 Eligibility

The following are eligible for license to operate as a switching company:

1. Deposit Money Banks
2. Consortium of Banks
3. Agent of a bank or banking consortium, ***subject to the provisions in section 1.4***
4. Any other company approved by the CBN

1.3.2 Parties to Switching Services

Parties to Switching Services include but not limited to:

1. Central Switch
2. Switching Companies
3. Deposit Money Banks
4. Other Financial Institutions
5. Independent Service Operators (ISO)
6. NIBSS
7. Merchants
8. Cardholders

9. Card Issuers
10. Merchant Acquirers

1.4 Rights and Responsibilities of a Switching Company

A switching company shall:

1.4.1 Operate its switch in accordance with the license issued to it

1.4.2 Ensure compliance with minimum standards on switches issued by the CBN and as amended from time to time

1.4.3 Open its network for reciprocal exchange of transactions/messages between it and the Central Switch

1.4.4 Shall enter into agreement with member institutions, specifying in clear terms the responsibilities of each party, operational rules and procedures and liabilities of parties in the event of loss of funds arising from negligence of any of the parties and a copy shall be submitted to the CBN for record

1.4.5 Ensure that all notifications and information that its employees have obtained in the course of discharging their responsibilities are treated as confidential

1.4.6 Establish adequate security procedures to ensure the safety and security of its information and those of its clients, which shall include physical, transactions, logical, network and enterprise security

1.4.7 Submit to the CBN its security plans and periodic updates. Any security breach shall have a record and such instances shall be reported to the CBN for record purpose

1.4.8 Charge fees for the services provided in relations to its respective switching network

1.4.9 Have a robust Business Continuity Plan approved by the CBN

1.4.10 Ensure full compliance with relevant provisions of the electronic banking and other guidelines issued by the CBN in relation to its operations

1.4.11 Not be an issuer of payment cards

1.4.12 Supply to the CBN, information on usage, volume and value of transactions and other relevant information, as and when due, and in the format required by the CBN

1.4.13 Maintain database on information relating to cardholders, merchants and their transactions for a minimum period of ten (10) years and in compliance with section 2.2.4

1.4.14 Report all instances of fraud/attempted fraud ***on the switch*** to the CBN

1.4.15 Have a primary site, hot backup site and contingency site as minimum requirement

1.4.16 Maintain a hot list of cards reported by member banks as lost, missing, stolen or damaged ***for the period of validity of the card***.

1.5 Rights and Responsibilities of Member Institutions

1.5.1 Member Institutions/Acquirers shall enter into contract with merchants for accepting payment by means of electronic payment instrument

1.5.2 Upon receipt of settlement from the acquirers, banks shall be responsible to the merchants for crediting their accounts with the amounts resulting from the operations on the principles and within the periods as specified in the contract referred to in 1.5.1

1.5.3 Member Institutions shall act as the issuer of payment cards and by so doing commit themselves towards the cardholders to settle the operations performed by means of payment cards, and the cardholder commits himself to pay the amount of the operations together with charges due to the issuer from a specified account.

1.5.4 The card shall be issued after signing the contract for payment card. Up to the moment of issuance, the issuer bears the responsibility for any ***fraud*** resulting from using the card by any unauthorized user

1.5.5 Upon receipt of payment card ***or card details and PIN*** by the holder, the holder bears the responsibility for any ***fraud*** resulting from using the card.

1.5.5 Acquirers whose transactions are switched shall maintain databases that can handle information relating to cardholders, merchants and their transactions for a minimum period of ten (10) years

1.5.6 Information on usage, volume and value of transactions and other relevant information shall be forwarded to the CBN as and when due and in the format required by the CBN

1.5.7 Each member institution shall settle fees charged for the services provided by the switching company in relation to the operation of the switching network, in accordance with the agreed tariff

1.5.8 Member Institutions shall enter into agreement with cardholders specifying in clear terms their responsibilities in terms of PIN protection and other security measures

1.5.9 Only licensed deposit taking institutions shall with the approval of CBN serve as the issuers of multi purpose payment card

1.5.10 The issuer shall be held liable (where proven) for frauds with the card arising from card skimming or other compromises of the issuer's security system.

1.5.11 Each member institution shall notify the switching company of card reported lost, stolen, damaged etc for the purpose of placing it on hot list

1.5.12 No card issuer or its agent shall deliver any card in a fully activated state

1.5.13 A card issuer shall put in place adequate credit controls to track and minimize credit fraud

1.5.14 No card issuer or its agent shall bill or charge a customer for an unsolicited card unless and until after the card is fully activated by cardholder.

1.5.15 No card issuer or its agent shall engage in the use of unethical tactics when marketing its card products to members of the public

1.5.16 No card issuer or its agent shall communicate false or misleading information regarding card terms and conditions, service fees/waivers, and/or associated promotions/gifts/prizes to members of the public

1.5.17 A card issuer must 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***
- ***Billing cycles***
- ***Termination procedures***
- ***Default/recovery procedures***
- ***Loss/theft/misuse of card procedures***
- ***Grievance/Complaints procedures***

1.5.18 A card issuer shall provide means whereby its cardholders may at any time of the day or night notify the loss, theft or fraudulent use of the card and the card issuer shall take all necessary steps to stop any further use of the affected card.

1.5.19 A card issuer shall keep sufficient internal records over a minimum ten (10) year period, and in line with existing CBN guidelines on Electronic Banking, to enable the tracing of errors on card-related transactions

1.5.20 An acquirer shall be responsible for ensuring that merchants put in place reasonable processes and systems for confirming payee identity and detecting suspicious or unauthorized usage of electronic payment instruments both where customer/card is physically present at point of sale or in cases where customer/card is not physically present like in Internet/web and telephone payment systems/portals.

1.5.21 No member institution shall issue or support the issuance of a card or access device that is restricted to only certain terminals/payment devices that have distinctive hardware and/or software features unless such terminals/payment devices are for use only in closed systems that are not normally made available to members of the general public.

1.6 Rights and Responsibilities of the Merchant

1.6.1 A merchant shall enter into agreement with an acquirer specifying in clear terms the obligations of each party.

1.6.2 An acquirer shall be responsible for crediting the account of the merchant with the amount resulting from operations, within periods as specified in the agreement, but not exceeding 3 days for online transactions and 5 days for offline transactions.

1.6.3 A merchant may refuse to accept payment by means of an electronic payment instrument, ***including payment with cards,*** if:

- The electronic payment instrument is invalid;
- Obtaining acceptance for execution of operations is not possible;
- Notification of loss, missing, stolen or damaged has been made of the electronic payment instrument;

- The cardholder refuses to present a document confirming his/her identity in the event of suspicious / unauthorized use of electronic payment instruments;

1.6.4 Each merchant shall be entitled to promptly receive from the issuer an updated list of cards that have been placed on the hot list.

1.6.5 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

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

1.6.7 A merchant shall neither practice differential pricing based on payment mode nor discriminate against any member of the public who chooses to pay with a card or by other electronic means. The prices of goods and services payable by any customer shall not be different regardless of the mode of payment.

1.7 Rights and Responsibilities of the Cardholder

1.7.1 Cardholder shall:

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

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

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

1.7.4 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.

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

1.7.6 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

1.7.7 The cardholder shall be entitled to receive, within a reasonable period or at an agreed intervals, a statement of all transactions is performed with his/her card

1.7.8 The cardholder shall be given reasonable notice before changes are made to fees levied on his/her card and be given the option to discontinue usage of card to avoid such changes in fees without penalty

1.7.9 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

1.7.10 The cardholder shall be entitled to privacy and information on his card account cannot be shared with third parties unless

- ***with express customer approval or***
- ***in cases of customer default, where information can be shared with credit bureaus and collection/recovery agents or***
- ***in cases where information is requested by valid order of a competent Nigerian court/authority or***
- ***in cases where it is necessary to prevent fraud***

1.8 Rights and Responsibilities of the Central Switch

The Central Switch shall:

1.8.1 be licensed by the CBN

1.8.2 be independent of other switching companies

1.8.3 not own or promote any card business or retails products and shall be run in accordance with international best practice

1.8.4 connect with all ***new and existing switching companies*** that meet its requirements for participation and have obtained the necessary license from the CBN

1.8.5 Enter into a written agreement with switching companies, specifying in clear terms the responsibilities of each party, and operational rules and procedures and copy shall be submitted to the CBN.

1.8.6 Ensure that all notification and information that its employees have obtained in the course of discharging their responsibilities shall be treated confidentially

1.8.7 Establish adequate security procedures to ensure the safety and security of its information and those of its clients, which shall include physical, transaction, logical, network and enterprise security

1.8.8 Charge fees for the services provided in accordance with agreement reached under sub-guideline ***1.8.5***

1.8.9 Have a robust Business Continuity Plan approved by the CBN

1.8.10 Ensure full compliance with all the relevant provisions of electronic banking guidelines and other guidelines issued by the CBN, from time to time

1.8.11 Supply information on usage, volume and value of transactions and other relevant information to the CBN as and when due and in the format required by the CBN

1.8.12 Maintain database on information relating to cardholders, merchants and their transactions for a minimum period of ten (10) years.

1.8.13 Report all instances of fraud / attempted fraud to the CBN

1.8.14 Have primary site, hot backup site and contingency site as minimum requirement

2.0 Technical Requirements/Standards

2.1 The central switch/switching companies and their member institutions shall ensure compliance with the following minimum standards:

- Minimum Standards for Messaging/Communication
- Minimum Standards for interoperability
- Minimum Security Standards
- Minimum Standards for Devices
- EMV Compliance Certification
- Minimum Standards for Card Design

2.2 The Central Switch and Switching Companies shall:

2.2.1 conduct half-yearly planned system tests to ensure ability to seamlessly switch from primary to back-up systems. Such tests shall

be communicated in advance to all member institutions and the CBN. These tests shall take place at times during the week and day when the least amount of network traffic occurs in order to minimize impact on customer service. The results of the tests shall be shared with all member institutions and the CBN within 3 business days.

2.2.2 publish a weekly report of all downtimes experienced to all member institutions and the CBN. Such reports shall include the duration of the downtime, the cause(s) of the downtime, and the remedial actions taken to prevent recurrence

2.2.3 ensure that all devices/software used for transmitting financial data within their switching networks are EMV 4.0 - Levels 1 & 2 compliant (or any newer EMV version as periodically advised by the CBN) by September 30, 2009

2.2.4 be in regular compliance with PCI Data Security Standards (DSS) by September 30, 2009

2.3 The central switch shall, subject to CBN approval and in consultation with member institutions, maintain minimum technical standards on interoperability, messaging, network connectivity, network monitoring, security, disaster recovery, fraud management, and programming interfaces

2.4 An acquirer/member institution shall be responsible for deploying terminals/payment devices that are EMV 4.0 - Levels 1 & 2 compliant (or any newer EMV version as periodically advised by the CBN). This guideline only affects new equipment purchases made after September 30, 2009

2.5 An acquirer/ member institution shall be responsible for deploying terminals/payment devices with PIN Entry Devices (PED) that are PCI Security Standards Council (SSC) PED complaint. This guideline only affects new equipment purchases made after September 30, 2009

2.6 The central switch shall maintain a list of approved network/link service providers. All connecting switches are required to maintain a minimum of two (2) network/link service providers as the primary and secondary link.

2.7 The central switch shall stipulate the minimum network/link bandwidth that must be provided by each network/link provider

2.8 The central switch shall stipulate the network/link standards and specifications for all equipment provided by each network/link provider at all terminating points

2.9 All switches have the duty to transmit all messages or financial transactions emanating from the Central Switch to their expected destinations without regard to the originating switch of such message or financial transaction.

2.10 No switch shall reject, degrade, give lower priority or service, or in any way negatively affect any message or financial transaction originating from the Central Switch

2.11 All switches shall connect to the Central Switch by July 30, 2009

3.0 Operational Rules and Procedures

3.1 Types of Transactions

The central switch/switching companies shall only handle switching services in accordance with the license issued to them.

3.2 Operating Hours

3.2.1 The central switch/switching companies shall operate 24 hours a day and 7 days a week

3.2.2 In case of system failure, the central switch / switching companies shall automatically switch to its / their back-up site (s)

3.3 Settlement Mechanism

3.3.1 The Central Switch shall work out the daily net settlement positions of member institutions and forward same through NIBSS to the CBN for settlement

3.3.2 Member Institutions shall provide adequate collaterals***, as deemed sufficient by the CBN,*** in form of Federal Government Securities in line with their contract agreements with Switching Companies.

3.3.3 ***Alternatively, member institutions may utilize existing cheque clearing collaterals held with the CBN to meet the collateral requirement for transaction switching mentioned in 3.3.2 above.***

3.3.4 The CBN shall effect the posting of the net settlement positions of member institutions into their accounts.

3.4 Incomplete/Irregular Transactions

In the event of irregularities in the account of card holder arising from the operations of electronic payment instrument, the following procedures shall apply:

3.4.1 The cardholder ***or any other party to the transaction*** shall immediately notify the issuer on irregularities in his account concerning:

- Contested transactions
- Understatement or overstatement of his account
- Debit in his account without obtaining the value for the transactions
- Other irregularities

3.4.2 The cardholder's notification shall be considered and verified without delay

3.4.3 Upon confirmation of the irregularities, the anomaly shall be corrected within a maximum period of 14 days ***from the date of settlement***.

3.4.4 Failure to regularize the anomaly within 14 days shall attract penalty on the defaulting party at the prevailing MPR

3.4.5 All related costs arising from the transaction shall be borne by the defaulting party.

3.5 Fraudulent Transactions

In the event of fraudulent transactions, the following procedures shall apply:

- The cardholder shall bear the cost of operations performed by persons, to whom he made available the payment card or disclose his PIN

- The cardholder shall bear the cost of operations performed by means of a lost payment card up till the time of notifying the issuer about the loss

- The cardholder shall not bear the cost of operations performed by means of his lost card, if this performance took place in consequence of defective execution of obligations by the issuer or merchant

3.6 Fees and Charges

3.6.1 Fees and charges for transactions switching, processing, etc are to be agreed between service providers and banks / entities to which the services are being provided.

3.6.2 Fees and charges for transaction switching shall not exceed predefined ceiling specified in 3.6.1 as may be reviewed from time to time.

3.7 Termination.

3.7.1 Member Institutions may terminate participation in the switching network by notifying the switching company at least one month prior to the intended termination date.

3.7.2 The switching company may suspend or terminate the participation of any member institution from the system by giving at least one month notice to the participating member, if the member institution is in breach of member institutions rules and responsibilities.

3.8 Special Provision

3.8.1 The central switch/switching companies and their members shall be required to undertake measures to prevent the use of their networks for purposes associated with money laundering and other financial crimes.

3.9 Penalties

A) Sanctions, in the form of monetary penalties of not less than N5 million and / or suspension of the specific switching service (s) or both, would be imposed on erring switching companies and / or their member institutions for failure to comply with any of the provisions of these guidelines and other relevant guidelines issued by the CBN from time to time.

Appendix 1: Definition of Terms

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

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

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

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

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

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

f) 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.

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

h) 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;

i) MPR means Minimum Policy Rate

j) 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.

k) 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.

l) 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.;

m) PIN means Personal Identification Number

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

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

p) 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

q) 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