

GUIDELINES

ON

**INTERNATIONAL MOBILE MONEY
REMITTANCE SERVICE**

IN

NIGERIA

Table of Content

	Page
1. Introduction	3
2. Objectives	3
3. Scope	4
4. Operations Of International Mobile Money Remittance Services (IMMRS) in Nigeria.	4
5. Authority to Provide International Mobile Money Remittance Services in Nigeria.	5
6. Business Rules	6
7. Roles and Responsibilities of Participants	7
8. Nominee/Settlement Account	10
9. Settlement	11
10. Transaction Security Standards	12
11. Infrastructure	14
12. Risk Management	15
13. Know Your Customer (KYC) and Customer Due Diligence (CDD) Requirements	18
14. Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT)	18
15. Consumer Protection Measures	19
16. Cessation of International Mobile Money Remittance Service	20
17. Statutory Returns	20
18. Remedial Measures	21
19. Sanctions	21
20. Review of Guidelines	21
21. Glossary of Terms	22



1.0 INTRODUCTION

Following the widespread use of mobile telephone as a means of communication in Nigeria, and in recognition of its potential as a tool for financial inclusion and efficient payments system, the Central Bank of Nigeria (CBN), pursuant to its powers under Section 47(2) of the CBN Act, 2007, issued the "Guidelines on Mobile Money Services in Nigeria" in 2009. The above guidelines, however, restricts users and operators of mobile payments services to local currency transactions within Nigeria. Also, the extant CBN "Guidelines on International Money Transfer Services in Nigeria" issued in June 2014 did not cover money remittances via mobile applications.

Consequent upon representations by some stakeholders on the need to facilitate foreign exchange transactions via a more convenient and flexible payment channel, the CBN has approved the inclusion of mobile money as part of international money transfer services in Nigeria. It is in this regard that the Bank hereby issues the "Guidelines on International Mobile Money Remittance Service (IMMRS) in Nigeria" to complement the existing guidelines.

These guidelines cover the business rules governing the operation of IMMRS and specify the infrastructural and risk management requirements for international mobile payments services in Nigeria. It also identifies the participants, and defines their expected roles and responsibilities in the system. In addition, it sets the basis for the regulation of services offered by the participants.

2.0 OBJECTIVES

The objectives of these guidelines are to:

- i. Provide minimum standards and requirements for the operation of



- international funds remittance over mobile devices in Nigeria;
- ii. Specify delivery channels for offering international funds remittance over mobile (inbound/outbound), in a cost effective manner;
 - iii. Provide an enabling environment for International funds remittance over mobile devices in the Nigerian economy;
 - iv. Specify minimum technical and business requirements for various participants in the International Funds Remittance over mobile devices in Nigeria; and
 - v. provide broad guidelines for implementation of processes and flows of international money transfer services, from initiation to completion.
 - vi. Ensure a structured and orderly development of International Funds Remittance over mobile devices in Nigeria, with clear definition of various participants and their expected roles and responsibilities.
 - vii. Promote safety and effectiveness of mobile money services and thereby enhance user confidence.

3.0 SCOPE

To achieve the above stated objectives, these Guidelines cover business rules, agent network, roles and responsibilities of participants under the scheme.

4.0 OPERATIONS OF INTERNATIONAL MOBILE MONEY REMITTANCE SERVICE (IMMRS) IN NIGERIA

4.1 Permissible Activities

The permissible activities of International Mobile Money Remittance Service (IMMRS) shall consist of allowable inbound and outbound transactions as follows:

(A) Inbound Remittances

The transaction shall be limited to the receipt of monies transmitted via mobile phones and other hand held devices to persons resident in Nigeria



and foreign visitors.

(B) Outbound Remittances

This includes all outbound Person-to-Person money remittances from Nigeria towards family maintenance. To safeguard against circumventing the statutory reporting threshold, the mobile money remittance service shall target individual customers only.

5.0 AUTHORITY TO PROVIDE INTERNATIONAL MOBILE MONEY REMITTANCE SERVICE IN NIGERIA

Institutions seeking to offer international mobile money remittance service in Nigeria shall apply and obtain a valid approval from the CBN subject to the following conditions;

- a. Be a registered entity, licensed in its home country to carry on money transfer activities.
- b. Have a minimum Net Worth of US\$1 billion, as per the latest audited financial statement, or as may be determined by the CBN from time to time.
- c. Should hold a valid Mobile Money Operator's license
- d. The Institution should be well established (operate in at least twenty countries with at least 10 years experience) in the money transfer business, with a track record of operations.
- e. There should be an MOU that clearly delineates liabilities in the event of disputes and/or process failures.

For operation of this service there must be in partnership with at least an Authorised Dealer bank licensed in Nigeria shall be eligible for the grant of CBN approval under these guidelines.



5.1 RESERVE RIGHTS OF THE CENTRAL BANK OF NIGERIA

The Central Bank of Nigeria shall have the right to decline the issuance of any license without any reason.

6.0 BUSINESS RULES

6.1 Requirements

All financial institutions authorised to carry out international mobile money remittance service in Nigeria shall:

- i. Be issued a unique Scheme Code by the NIBSS for managing interoperability.
- ii. Be issued unique short codes by the NCC.
- iii. Ensure that all telecommunication equipment is type approved by the NCC.
- iv. Register users of its scheme based on technology standards and the requirements of these Guidelines.
- v. Ensure that the registration processes within its International Funds Remittance scheme shall fulfil the entire KYC requirements specified in these Guidelines.
- vi. Display the summary of transaction requested to the user for confirmation which shall include the phone numbers of the initiator and receiver, transaction description, the transaction amount, date and time and a unique transaction identifier.
- vii. The user commits to the transaction by confirming the summary.
- viii. Provide the user option to save transaction summary.
- ix. Ensure upon completion of the transaction, that the user receives an electronic confirmation.
- x. Regulatory authorities shall have access to the transaction log.
- xi. Ensure that all transfers are subjected to the sanction screen platform



6.2 Activation

- (a) All banks offering international funds remittance over mobile devices shall provide an Application, which shall require a registered user to activate the service before the commencement of transactions with a security code (e.g. PIN/Password, etc.).
- (b) The bank shall ensure that the activation process is not compromised or altered within its infrastructure.

6.3 Transactions

- (a) All transactions within the IMMRS shall have a unique reference issued by the system.
- (b) All transactions shall have; reference number, payer and payee phone numbers, amount, unique identifier date and time and other relevant transaction details.
- (c) IMMRS providers shall appoint and notify CBN of their settlement/correspondent banks.

6.4 International Mobile Money Remittance Payments Processes

The IMMRS shall put in place detailed processes that cover the entire solution delivery, from user registration and management, consumer protection, dispute resolution procedures, risk management processes, to transaction settlement.

7.0. ROLES AND RESPONSIBILITIES OF PARTICIPANTS

7.1 Banks

The role/responsibilities of banks as Scheme Operators shall include:

- (a) Verification, approval and accountability for the credibility and integrity of their partner organizations.



- (b) Seeking and obtaining necessary approvals from relevant regulatory authorities.
- (c) The deployment and delivery of the International Funds Remittance over mobile payment services to the customer.
- (d) Ensuring that the International Funds Remittance over mobile payment service meets all specified mobile payment standards as provided in this Guidelines.
- (e) Putting in place adequate measures to mitigate all the risks that could arise in the use of its mobile payment service.
- (f) Facilitating remittances to both scheme and non-scheme recipients.
- (g) Providing financial, clearing and settlement services to the mobile payments system.
 - (h) Educating the customers on the appropriate use of the service and ensuring the deployment of adequate channels for enquiries and complaints.

7.2 Infrastructure Providers

These are organizations providing infrastructure that enable switching, processing and settlement facilities for International Funds Remittance over mobile services. Settlement here refers to Foreign Exchange Settlement.

7.3 Mobile Network Operators (MNOs):

Their role shall be guided by the following provisions:

- (a) Providing telecommunication network infrastructure for the use of International Funds Remittance over Mobile devices;



- (b) Ensuring that a secure communication channel based on the minimum technology standard stipulated in these Guidelines are implemented;
- (c) That MNOs shall not give preferential treatment to any mobile money operator over another in terms of traffic and price;
- (d) Ensuring that its customers are free to use any mobile payments scheme service of their choice;
- (e) Shall not receive deposits from the public, except in respect of the airtime billing of their customers;
- (f) Shall not allow the use of the airtime value loaded by their customers for purposes of payments or to transfer monetary value;
- (g) Shall ensure seamless interconnection between MMOs; and
- (h) Shall not engage in any conduct which has a purpose or effect of anti-competition in any aspect of mobile money services.

7.4 Consumers

They shall have rights/responsibilities as follows:

- (a) Ease of enrolment
- (b) Ease of use (SMS, USSD, STK, IVR, etc.)
- (c) Privacy, Trust and Security of transaction
- (d) Convenience
- (e) Accessibility to funds on completion of transaction process
- (f) Real time transfer of value



- (g) Easy and prompt access to dispute resolution process
- (h) Ensure the protection of PIN / Password
- (i) Ensure prompt reporting of fraud cases, errors and complaints
- (j) Ensure proper confirmation of transaction details and recipients' mobile phone numbers at all times before authorizing transactions.
- (k) Comply with all security rules as provided by the scheme operator
- (l) Report complaints to the Consumer Protection Departments of the Central Bank of Nigeria, if resolution exceeds 14 working days.

8.0 NOMINEE/SETTLEMENT ACCOUNT

- (a) IMMRS providers shall notify CBN of their settlement/correspondent banks.
- (b) All obligations arising from mobile money transactions shall be settled into settlement accounts.
- (c) The settlement accounts with the deposit money banks shall be opened as Nominee Accounts on behalf of the customers of the international Mobile Money Service providers. The operations of the account shall be guided by the following conditions:
 - i. no right of set-off,
 - ii. debit transactions into the account shall only be for settlement related transactions
 - iii. No charges of any form shall apply to the account
- (d) The settlement account shall not be used, under any guise or purpose, as collateral for negotiation of loans by the bank.



- (e) The balance on the settlement account shall always be equal to the total outstanding (un-spent) balance of all holders of the mobile money.
- (f) International Mobile Money Service Providers shall be required to reconcile on a daily basis, the balances in their pool accounts and make monthly returns to the Director, Trade & Exchange Department of the CBN.
- (g) All customer transactions shall be traceable; auditable and can be validated.
- (h) Remittance inflow messages shall, at a minimum, be conveyed to the recipient through SMS.

9.0 SETTLEMENT

- a. The settlement process to be deployed by International Mobile Money Remittance Service providers shall ensure compliance with the settlement standards and requirements defined in these Guidelines.
- b. The IMMRS provider shall ensure that its mobile payment infrastructure fully complies with the clearing and settlement rules for finality of settlement.
- c. The scheme operator shall, on a daily basis request for its settlement positions from its correspondent bankers for reconciliation of transactions.
- d. The scheme operator shall ensure that all settlement information details are preserved for reference for a minimum period of seven (7) years.

9.1 Operating Rules for Scheme Settlement Operator

Nigeria Inter-bank Settlement System Plc (NIBSS) shall:

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

- (b) Provide statistical reports to the regulatory bodies and participants as may be prescribed from time to time
- (c) Maintain audit trail and transaction log of all transactions consummated on the scheme.
- (d) Provide the infrastructure (hardware, software, switching and security) to link all inter scheme providers.
- (e) Provide business continuity/disaster recovery plans to ensure services are available at all times.
- (f) Provide 99.99% system availability and ensure that all signed-on participating institutions follow same rules.
- (g) Ensure MMOs are connected to the National Central Switch (NCS) for the purpose of interoperability.
- (h) Ensure that the mobile payments system is interoperable with the network infrastructure of different MNOs, solution providers, IMMRS and the NCC.

10.0 TRANSACTION SECURITY STANDARDS

10.1 Mobile Payments solutions deployed shall adhere to the following minimum standards:

- (a) The Advanced Encryption Standard (AES). Encryption shall be on an end-to-end basis.
- (b) ISO 8583
- (c) All subsequent routing of messages to the Mobile Money Operators' servers must be with the highest level of security with dedicated connectivity;
- (d) That any sensitive information stored in third party systems is restricted with appropriate encryption and hardware security standards as contained in this guidelines;
- (e) All transactions on an account shall be allowed only after authentication of the mobile number and the PIN associated with it;

- (f) That mobile payments application shall not allow the option of saving the PIN either on the handset or on the application;
- (g) All accounts on the mobile application shall be activated using the costomer on the mobile application linked to the mobile phone number. This mobile phone number shall be used as the second factor authentication for mobile transactions;
- (h) The PIN shall not travel in plain text during the transaction;
- (i) That proper system of verification of the phone number shall be implemented;
- (j) The payment authorisation message from the user's mobile phone shall, at the minimum, be AES encrypted and checked for tampering by the scheme operator. It shall not be possible for any interceptor to change the contents of the message;
- (k) There shall exist, a security policy duly approved by the Board of Directors of the organisation providing the service;
- (l) Segregation of duty of Security Officer / Group dealing exclusively with information systems security and Information Technology Division which actually implements the computer systems;
- (m) The Information Systems Auditor shall conduct periodic audit of the system to ensure adherence to the specified security standards half yearly;
- (n) Logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. exists;
- (o) At the minimum, there shall be in place, the use of proxy server type of firewall so that there is no direct connection between the Internet and the Mobile Money Operators' systems. For sensitive systems, an inspection firewall shall

be implemented to thoroughly inspect all packets of information, compare past and present transactions and enable a real time security alert;

11.0 INFRASTRUCTURE

The core infrastructure for providing an international mobile payment system shall comply with the following standards and other requirements outlined in these guidelines:

a. Standards

- i. Transaction processing, clearing and settlement platforms.
The responsibility for the provision and management of these platforms shall be that of the bank.
- ii. The IMMRs shall ensure that the minimum technology standards for communication are met (Interoperability and Interconnectivity).
- iii. Only secure channels shall be used in providing mobile money services
- iv. The mobile money services shall ensure non-repudiation.

b. Reliability

- i. Payment instruction shall be consistently executed. In the event of failure, reversal shall be immediate and automatic.
- ii. Consumers shall get immediate value for every successful transaction.

c. User Interface

- i. The user interface shall, at the minimum, adhere to the security requirements as stated in the guideline.
- ii. The user interface shall not provide access to confidential information.
- iii. PIN shall be encrypted at the point of entry.



12.0 RISK MANAGEMENT

12.1 In view of the peculiarity of the operations of the IMMRS and the unique risks associated with their operations, these guidelines hereby specifies the following minimum requirements to management of risks arising from their activities.

- (a) The IMMRS shall ensure that risk management policies are in place to minimize operational, liquidity, settlement, fraud, financial and money laundering risks.
- (b) The mobile payments system shall not be susceptible to sustained operational failures, as a result of system outages.
- (c) A risk management officer shall be assigned by the IMMRS, who is to provide internal risk management oversight.
- (d) The CBN will review the risk management policies, including all the controls that are in place to manage the risks from time to time.
- (e) Without prejudice to the existing enterprise Risk management framework in the bank, emerging risks from the deployment of this service should be submitted to the Central Bank of Nigeria for review and approval as part of the licensing process



12.2 Credit and Settlement Risk

The central role of the settlement infrastructure requires that IMMRS shall:

- (a) Ensure that the mobile payment settlement platform automatically generates transaction settlement information/records.
- (b) Maintain audit trail and settlement log for a minimum of seven (7) years.
- (c) Fulfill other conditions that may be reviewed by the regulatory authorities from time to time.

12.3 Business Continuity Plan (BCP)

IMMRS shall:

- (a) Ensure that BCP is approved by their board.
- (b) Comply with laid down minimum technology standards as specified in this document.
- (c) Ensure proper/adequate back up of data as may be required by their operations.
- (d) Ensure that the BCP is tested through a fail-over process, at least twice a year.
- (e) Have, well documented and tested business continuity plans approved by the board, that address all aspects of the mobile payment business, to take care of business disruptions and ensure system availability and recoverability:
 - i. data should be backed up daily while software should updated as appropriate



- ii. Recovery and business continuity measures, based on the criticality of the systems, shall be in place and a documented plan with the organization and assignment of responsibilities of the key decision making personnel shall exist.
- iii. An off-site back up is required for recovery from major failures / disasters to ensure business continuity. Different technologies based on backup, hot sites, warm sites or cold sites should be available for business continuity.

12.4 The BCP shall be:

- (a) Based on a comprehensive Business Impact Analysis and Risk Assessment;
- (b) Documented in a written format;
- (c) Reviewed and approved by the board and senior management, at least annually;
- (d) Disseminated to employees;
- (e) The responsibility of the IMMRS, where it is outsourced to a third-party;
- (f) Flexible to respond to unanticipated threat scenarios and changing internal conditions;
- (g) Focused on the impact of various threats that could potentially disrupt operations rather than on specific events;
- (h) Developed based on valid assumptions and an analysis of interdependencies;
- (i) Effective in minimizing service disruptions and financial loss through the implementation of mitigation strategies.



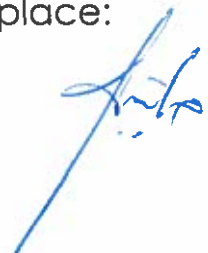
- (j) Ensure that processing priorities can be adequately implemented and that business operations resumes within twenty-four (24) hours.
- (k) Monitor closely mobile traffic and system capacity to ensure that any service degradation due to capacity problems are addressed promptly.
- (l) Ensure that the BCP is reviewed by external auditors at least annually, and forwarded to CBN;
- (m) Ensure employees are trained and aware of their roles in the implementation of the BCP;
- (n) Ensure the BCP is tested, at least quarterly, on an enterprise-wide basis;
- (o) Review the BCP testing program and test results on a quarterly basis;
- (p) Ensure the BCP is continually updated to reflect the current operating environment.

13.0 KNOW YOUR CUSTOMER (KYC) AND CUSTOMER DUE DILIGENCE (CDD) REQUIREMENTS

All IMMRS shall comply with the provisions of the KYC Guidelines (CBN AML/CFT Regulation 2013).

14.0 Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT)

The IMMRS providers shall have measures in place to prevent money laundering and terrorist financing. The mobile money IT system shall have inbuilt mechanisms to identify suspicious transactions. The following measures shall be in place:



- (a) Adhere to international Know Your Customer (KYC) standards at account opening by carrying out Customer Due Diligence (CDD). The entity conducting customer verification should require at least one of the following documents to verify the identity of the customer: a valid international passport, National Identity card, permanent voter's card, driver's license.
- (b) Allowable maximum limit of the outbound mobile money remittance per week shall be US\$100 or its equivalent, subject to periodic review by the CBN.
- (c) Suspicious transactions should be reported in line with the AML/CFT Act.

15.0 CONSUMER PROTECTION MEASURES

IMMRS shall comply with the following minimum requirements:

- a. Ensure that customers understand the transactions they are entering and adequate disclosures are made.
- b. Ensure that a channel of communication is in place twenty four (24) hours a day, seven (7) days a week to entertain enquiries and complaints in a language understood by customers.
- c. Clearly display charges for services rendered.
- d. Factor in the vulnerability of the lower end of the society in product and services design. There should be adequate consumer education activities to ensure that consumers are sensitized on the services.
- e. Ensure that appropriate consumer protection mechanisms are put in place against loss of service, fraud and privacy of customer information to enhance confidence in the mobile money services.
- f. Provide the leading role in dispute resolutions and take necessary steps to reach other agencies in the ecosystem that are relevant to resolving disputes.



- g. Respond to customer complaints within a reasonable time and not later than 48 hours from the date of reporting or lodging the complaint with the IMMRS.
- h. Be held responsible for the actions and inactions IMMRS.

15.1 DISPUTE RESOLUTION MECHANISMS

Disputes arising between parties shall be settled as follows:

- a. The parties shall settle disputes within 14 working days.
- b. Customers may report complaints addressed to the Director, Consumer Protection Department Central Bank of Nigeria where they are dis-satisfied with item a above.
- c. If resolution is not achieved, after (a & b) above, parties may thereafter settle the dispute in accordance with the provisions of the Arbitration and Conciliation Act, Cap A18, Laws of the Federation of Nigeria, 2004 and other applicable legislations.

16.0 CESSATION OF MOBILE PAYMENT SERVICE

- a. Any IMMRS wishing to exit from the mobile payments system shall notify the CBN in writing regarding the intention for the discontinuation, 120 days before ceasing its operations;
- b. The CBN shall have powers to order any IMMRS exiting from the mobile payments system to meet its outstanding obligations.

17.0 STATUTORY RETURNS

IMMRS shall, at the end of every month and not later than the 10th day of the following month, submit to the CBN, data and other information on International mobile money operations including:

- i. Nature, value and volume of transactions;



- ii. Incidents of fraud; and
- iii. Nature and number of customer complaints and remedial measures taken.

17.1 Annual Reporting

IMMRS shall include in their annual reports and accounts, in the prescribed format all activities of its mobile money operations.

18.0 REMEDIAL MEASURES

If an IMMRS or its agent fails to comply with these Guidelines, the CBN may take any corrective action against the IMMRS as may be prescribed from time to time.

19.0 SANCTIONS

In addition to the use of remedial measures, the Bank may impose any or all of the following sanctions against an IMMRS, its board of directors, officers or agents:

- (a) Withholding Corporate approvals;
- (b) Financial Penalties;
- (c) Suspension from International mobile money operation; and
- (d) Revocation of the mobile money operation license.

20.0 REVIEW OF THE GUIDELINES

These Guidelines shall be reviewed from time to time by the Central Bank of Nigeria.



21.0 GLOSSARY OF TERMS

Bank: A deposit taking institution duly licensed by the Central Bank of Nigeria.

EMV: Europay, Mastercard and Visa (Chip and PIN)

Infrastructure Providers: These are organizations providing infrastructure that enable switching, processing and settlement facilities for mobile money services. Settlement here refers to Inter-Scheme Settlement.

International Mobile Money Remittance Service Providers: provide the infrastructure for the mobile payment systems for the use of participants that are signed-on to their scheme.

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

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

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

ISO8583: International Organisation Standard 8583 (messaging format)

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

Non-scheme recipients:



Nominee Account: Account set up by a Nominee (MMO) for settlement of customer transactions held on behalf of the individual customers (the 'beneficial owner') under a custodial agreement.

PCIDSS: Payment Cards Industry Data Security Standard

Settlement Infrastructure Providers: Organizations providing infrastructure that enables message exchange, switching and settlement facilities for mobile money services.

Scheme recipients:

AES: Advanced Encryption Standard

A handwritten signature in blue ink, appearing to be 'J. P. ...', located on the right side of the page.

"APPENDIX I"

APPROVAL REQUIREMENTS FOR INTERNATIONAL MOBILE MONEY SERVICE PROVIDERS

1. Evidence of the formation of the Consortium that will deploy the project (Certificate of Incorporation)
2. The Consortium's profile and functional contact e-mails and telephone numbers
3. Memorandum & Articles of Association
4. Shareholding structure of the Consortium
5. Forms C02 (Return on Allotment of shares) and C07 (Particulars of Directors)
6. CV's of Board and Management of the Company
7. Organogram of the company
8. Business Plan, to include:
 - a. Nature of the Business
 - b. Features of the scheme
 - c. Securities features that will be put in place
 - d. 3 years Financial projections for the company
 - e. Transaction and other charges that will be borne by customers
 - f. Profit sharing agreement among the parties
 - g. Diagrammatic illustration of transaction flows
9. Information Technology Policy of the Company including:
 - a. Privacy Policy
 - b. Information Ownership/Disclosure/Loss Policy
 - c. Backup and Restore Policy
 - d. Network Security Policy
 - e. Encryption Policy
 - f. Confidential Data Policy
 - g. Password Policy
 - h. Third Party Connection Policy



- i. Incidence Response Policy
 - j. Physical Security Policy
10. Enterprise Risk Management Framework
 11. Contingency and Disaster Recovery Plan (Business Continuity Programme)
 12. Draft agreements with the following:
 - a. Technical Partners
 - b. Participating banks
 - c. Switching company/(s)
 - d. Merchants
 - e. Telcos
 - f. Any other party
 13. Tax Clearance Certificate for three (3) years of each party in the Consortium
 14. Project Deployment Plan (time, location, operation, etc.)
 15. Payment of non-refundable Application fee of N1,000,000.00 (One million naira) made payable to the CBN via the RTGS Third Party Transfer.

