CENTRAL BANK OF NIGERIA

GUIDELINES ON ELECTRONIC BANKING IN NIGERIA

AUGUST, 2003

CENTRAL BANK OF NIGERIA

GUIDELINES ON ELECTRONIC BANKING IN NIGERIA

Preamble

The CBN recognizes that electronic banking and payments services are still at the early stages of development in Nigeria. Arising from the three major roles of the CBN in the areas of monetary policy, financial system stability and payments system oversight, the CBN Technical Committee on E-Banking has produced a report, which anticipates the likely impact of the movement towards electronic banking and payments on the achievement of CBN's core objectives. Following from the findings and recommendations of the Committee, four categories of guidelines have been developed as follows:

- Information and Communications Technology (ICT) standards, to address issues relating to technology solutions deployed, and ensure that they meet the needs of consumers, the economy and international best practice in the areas of communication, hardware, software and security.

- Monetary Policy, to address issues relating to how increased usage of Internet banking and electronic payments delivery channels would affect the achievement of CBN's monetary policy objectives.

- Legal guidelines to address issues on banking regulations and consumer rights protection.

- Regulatory and Supervisory, to address issues that, though peculiar to payments system in general, may be amplified by the use of electronic media.

The Guidelines are expected to inform the future conduct of financial institutions in e-banking and electronic payments delivery. A detailed report of the Technical Committee on e-Banking, which resulted in these Guidelines, is available separately.

THE GUIDELINES

1.0 Technology and Security Standards

CBN will monitor the technology acquisitions of banks, and all investments in technology, which exceed 10% of free funds, will henceforth be subject to approval. Where banks use third parties or outsource technology, banks are required to comply with the CBN guidelines.

1.1. Standards for Computer Networks & Internet

a. Networks used for transmission of financial data must be demonstrated to meet the requirements specified for data confidentiality and integrity.

b. Banks are required to deploy a proxy type firewall to prevent a direct connection between the banks back end systems and the Internet.

c. Banks are required to ensure that the implementation of the firewalls addresses the security concerns for which they are deployed.

d. For dial up services, banks must ensure that the modems do not circumvent the firewalls to prevent direct connection to the bank's back end system.

e. External devices such as Automated Teller Machines (ATMs), Personal Computers, (PC's) at remote branches, kiosks, etc. permanently connected to the bank's network and passing through the firewall must at the minimum address issues relating to non-repudiation, data integrity and confidentiality. Banks may consider authentication via Media Access Control (MAC) address in addition to other methods.

f. Banks are required to implement proper physical access controls over all network infrastructures both internal and external.

1.2. Standards on Protocols

Banks must take additional steps to ensure that whilst the web ensures global access to data enabling real time connectivity to the bank's back-end systems, adequate measures must be in place to identify and authenticate authorized users while limiting access to data as defined by the Access Control List.

Banks are required to ensure that unnecessary services and ports are disabled.

1.3. Standards on Application and System Software

a. Electronic banking applications must support centralized (bank-wide) operations or branch level automation. It may have a distributed, client server or three tier architecture based on a file system or a Database Management System (**DBMS**) package. Moreover, the product may run on computer systems of various types ranging from PCs, open systems, to proprietary main frames.

b. Banks must be mindful of the limitations of communications for server/client-based architecture in an environment where multiple servers may be more appropriate.

c. Banks must ensure that their banking applications interface with a number of external sources. Banks must ensure that applications deployed can support these external sources (interface specification or other CBN provided interfaces) or provide the option to incorporate these interfaces at a later date.

d. A schedule of minimum data interchange specifications will be provided by the CBN.

e. Banks must ensure continued support for their banking application in the event the supplier goes out of business or is unable to provide service. Banks should ensure that at a minimum, the purchase agreement makes provision for this possibility.

f. The bank's information system (IS) infrastructure must be properly physically secured. Banks are required to develop policies setting out minimum standards of physical security.

g. Banks are required to identify an ICT compliance officer whose responsibilities should include compliance with standards contained in these guidelines as well as the bank's policies on ICT.

h. Banks should segregate the responsibilities of the Information Technology (IT) security officer / group which deals with information systems security from the IT division, which implements the computer systems

1.4 Standards on Delivery Channels

1.4.1 Mobile Telephony: Mobile phones are increasingly being used for financial services in Nigeria. Banks are enabling the customers to conduct some banking services such as account inquiry and funds transfer. Therefore the following guidelines apply:

a. Networks used for transmission of financial data must be demonstrated to meet the requirements specified for data confidentiality, integrity and non-repudiation.

b. An audit trail of individual transactions must be kept.

***1.4.2 Automated Teller Machines* (ATM):** In addition to guidelines on e-banking in general, the following specific guidelines apply to ATMs:

a. Networks used for transmission of ATM transactions must be demonstrated to meet the guidelines specified for data confidentiality and integrity.

b.

c. In view of the demonstrated weaknesses in the magnetic stripe technology, banks should adopt the chip (smart card) technology as the standard, within 5 years. For banks that have not deployed ATMs, the expectation is that chip based ATMs would be deployed. However, in view of the fact that most countries are still in the magnetic stripe conversion process, banks may deploy hybrid (both chip and magnetic stripe) card readers to enable the international cards that are still primarily magnetic stripe to be used on the ATMs.

d. Banks will be considered liable for fraud arising from card skimming and counterfeiting except where it is proven that the merchant is negligent. However, the cardholder will be liable for frauds arising from PIN misuse.

e. Banks are encouraged to join shared ATM networks.

f. Banks are required to display clearly on the ATM machines, the Acceptance Mark of the cards usable on the machine.

g. All ATMs not located within bank premises must be located in a manner to assure the safety of the customer using the ATM. Appropriate lighting must be available at all times and a mirror may be placed around the ATM to enable the individual using the ATM to determine the locations of persons in their immediate vicinity.

h. ATMs must be situated in such a manner that passers by cannot see the key entry of the individual at the ATM directly or using the security devices.

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

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

k. Non-bank institutions may own ATMs, however such institutions must enter into an agreement with a bank for the processing of all the transactions at the ATM. If an ATM is owned by a non-bank institution, processing banks must ensure that the card readers, as well as, other devices that capture/store information on the ATM do not expose information such as the PIN number or other information that is classified as confidential. The funding (cash in the ATM) and operation of the ATM should be the sole responsibility of the bank.

l. Where the owner of the ATM is a financial institution, such owner of the ATM must also ensure that the card reader as well as other devices that capture information on the ATM does not expose/store information such as the PIN number or other information that is classified as confidential to the owner of the ATM.

m. ATMs at bank branches 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 within the hours of operations. Deployers are to take adequate security steps according to each situation subject to adequate observance of standard security policies.

n. Banks are encouraged to install cameras at ATM locations. However, such cameras should not be able to record the keystrokes of such customers.

o. At the minimum, a telephone line should be dedicated for fault reporting, and such a number shall be made known to users to report any incident at the ATM. Such facility must be manned at all times the ATM is operational.

1.4.3 Internet Banking

Banks should put in place procedures for maintaining the bank's Web site which should ensure the following:-

a. Only authorized staff should be allowed to update or change information on the Web site.

b. Updates of critical information should be subject to dual verification (e.g. interest rates).

c. Web site information and links to other Web sites should be verified for accuracy and functionality.

d. Management should implement procedures to verify the accuracy and content of any financial planning software, calculators, and other interactive programs available to customers on an Internet Web site or other electronic banking service.

e. Links to external Web sites should include a disclaimer that the customer is leaving the bank's site and provide appropriate disclosures, such as noting the extent, if any, of the bank's liability for transactions or information provided at other sites.

f. Banks must ensure that the Internet Service Provider (ISP) has implemented a firewall to protect the bank's Web site where outsourced.

g. Banks should ensure that installed firewalls are properly configured and institute procedures for continued monitoring and maintenance arrangements are in place.

h. Banks should ensure that summary-level reports showing web-site usage, transaction volume, system problem logs, and transaction exception reports are made available to the bank by the Web administrator.

1.4.4 Point of Sale Devices

a. Deployers of point of sale devices at merchant locations including where such companies are agents of financial institutions must familiarize the merchant location with the safe operation of the Point of sale device.
b. Private companies may deploy Point of Sale terminals, however such companies are required to sign agreements with banks that they are responsible to the merchant for transactions done on the terminals.
c. Acquiring banks must ensure that the Point of sale device as well as other devices that capture information do not expose/store information such as the PIN number or other information classified as confidential. It must also ensure that a customer's PIN number cannot be printed at the point of sale for any reason whatsoever.
d. Operators of point of sale devices are encouraged to work towards interoperability of cards from other schemes.

1.4.5 International Card Schemes: Banks may, subject to the approval of CBN, issue international cards (such as Visa, MasterCard etc.) to their customers. Such cards can be used wherever accepted, and payment on the cards can only be done through an ordinary domiciliary account of the cardholder, or any other account that may be permitted by the CBN. Banks may subject to the prior approval of the CBN acquire international cards for which the merchant receives value in Naira at the applicable rate at the CBN for the currency on the date of settlement. For domestic credit cards, transaction fees should be denominated in Naira.

1.4.6 Electronic Bill Presentment: Settlement should be done through the banking system. Third party (non bank) providers must first enter into agency agreement with financial institutions that will act as the settlement organization.

1.4.7 Switches: Since switches connect consumers to their bank accounts to authorize transactions, only banks or a consortium of banks or agents for a bank or banking consortium or any other company approved by the CBN can act as a switching company. Switching companies will be licensed as EFT Messaging Companies. This provision is to minimize fraud and mitigate risk to the banking system. Third party providers are to submit themselves to the scrutiny of the Central Bank only after having signed a switching agreement with a bank or consortium of banks. The switching companies must meet the standards defined in 3rd party service provider agreement. Third parties or service providers must meet the guidelines as specified by the CBN.

a. EFT companies and banks whose transactions are switched must maintain databases that are able to handle information relating to cardholders, merchants and bank transactions for no less than 180 days. In addition, they are required to preserve records of transactions for a minimum of five (5) years for audit purposes.
b. Switch operators must submit to the CBN their security plans and periodic updates. Any security breach must have a record and such instances should be reported to the CBN for collective solutions and future prevention.
c. Information on usage, volume of transactions and other relevant information should be supplied to the CBN on periodic basis for record purposes. In addition, information on instances of fraud and perpetrators should be reported to the CBN for record purpose.

d. In order to promote interoperability, all licensed switch operators are encouraged to inter-connect to each other.

1.4.8 **Internet Service Providers**: Internet Service Providers (ISPs) should exercise due diligence to ensure that only websites of financial institutions duly licensed by the CBN are hosted on their servers. ISPs that host unlicensed financial institutions would therefore be held liable for all acts committed through the hosted websites.

1.4.9 Cards Schemes: Cards can only be issued by deposit taking institutions duly licensed by the CBN, however where cards are used in a closed environment, such as telephone cards issued by a telephone company to its own customers or a fuel station issuing cards to its customers, this is permissible. Any such card issued in a closed environment should not be used for the exchange of value outside the closed group.

a. Banks must adopt a standard card numbering scheme. This is to ensure that cards issued by different banks are numbered in a unique manner, thereby preventing the possibility of two cards in the marketplace bearing the same card number.
b. The CBN will issue the first six numbers for each card issuing organization followed by a card numbering sequence chosen by the bank.
c. All cards must maintain a minimum of 9 digits and a maximum of twenty (20) characters. Banks that may consider the possibility of international acceptance of their cards must consider using a sixteen (16) digit numbering sequence.
d. The CBN will utilize ISO card numbering specifications and all cards therefore will be listed in the international registry of card issuers making cards and the issuers in Nigeria easily identifiable to the international community.

1.4.10 Electronic Transfer of Funds*:* Only authorized financial institutions can undertake electronic transfer of funds on behalf of customers.

a. Operators must ensure a safe and sound EFT network-switching environment, which with adequate internal controls, should minimize errors, discourage fraud and provide an adequate audit trail.
b. Operators must conduct periodic control and evaluations of the switch and the network and ensure daily settlement of switch activity and balancing of network activity. The Central Bank of Nigeria must be notified of fees charged as well as changes to the fees charged for services.
c. Management must ensure the existence of written and approved policies and procedures covering personnel, security controls, operations and disaster recovery, which must be enforced.
d. EFT Operators must conform to guidelines for security and privacy policies established by the Central Bank of Nigeria.

1.5. Standards on Security and Privacy

1.5.1 Security Policy and Privacy

Banks should have in place a security policy duly approved by their Boards, and the policy should address the following issues:

a. Basic approach to information security measures.

b. The ICT systems that must be protected and the reasons for such protection.
c. Priorities of information and information systems that must be protected.
d. Involvement and responsibility of management and establishment of an information security coordination division.
e. Checks by legal department and compliance with laws/regulations.
f. The use of outside consultants.
g. Identification of information security risks and their management.
h. Impact of security policies on quality of service to the customers (for example, disabling an account after three unsuccessful logins may result in denial of service when it is done by somebody else mischievously or when restoration takes unduly long time).
i. Decision making process of carrying out information security measures.
j. Procedures for revising information security measures.
k. Responsibilities of each officer and employee and the rules (disciplinary action, etc) to be applied in each case.
l. Auditing of the compliance to the security policy.
m. User awareness and training regarding information security.
n. Business Continuity Plans.
o. Procedures for periodic review of the policy and security measures.
p. Procedures for change and configuration management covering all facilities.

1.5.2 Standards on Identification

All users of critical devices on networks used for e-banking should to be uniquely identified to facilitate arrangements for authentication, access control, confidentiality demarcations and enforcement of security policies. A customer registration process primarily managed by a national root Certification Authority will ensure that all users and critical devices are uniquely identified and linked with all authorized identification systems (National Id, Passport, Driver's License, etc)

a. All identities must be aged and renewed on expiry.
b. Authentication: A minimum of two-factor authentication process is required for all user access to the services provided. Banks may need to consider the use of Public Key Infrastructure (PKI) for authentication of users for e-banking services.

1.5.3 Access Control: Banks should introduce logical access controls over ICT infrastructure deployed. Controls instituted by banks should be tested through periodic Penetration Testing, which should include but should not be limited to;

a. Password guessing and cracking
b. Search for back door traps in programs.
c. Attempts to overload the system using Ddos (Distributed Denial of Service & DoS (Denial of Service) attacks.
d. Check if commonly known vulnerabilities in the software still exist.
e. Banks may for the purpose of such Penetration Testing employ external experts.

1.5.4 Security Log (audit Trail): All computer accesses, including messages received, should be logged. All computer access and security violations (suspected or attempted) should be reported and follow up action taken as the organization's escalation policy.

a. *Log of Messages:* The banking applications run by the bank should have proper record keeping facilities for legal purposes.
b. All received and sent messages must be kept in both encrypted and decrypted form. (When stored in encrypted form, it should be possible to decrypt the information for legal purpose by obtaining keys with owners' consent.)

***1.5.5 Backup, recovery & business continuity*:** Banks should ensure adequate back up of data as may be required by their operations. Banks should also have, well documented and tested business continuity plans that address all aspects of the bank's business.

a. Both data and software should be backed up periodically, the frequency of back up depending on the recovery needs of the application. Online / real time systems require frequent backups within a day. The back-up may be incremental or complete. Automating the back up procedures is preferred to obviate operator errors and missed back-ups.
b. Recovery and business continuity measures, based on criticality of the systems, should be in place and a documented plan with the organization and assignment of responsibilities of the key decision making personnel should exist.
c. An off-site back up is necessary for recovery from major failures / disasters to ensure business continuity. Depending on criticality, different technologies based on back up, hot sites, warm sites or cold sites should be available for business continuity. The business continuity plan should be frequently tested.

1.6. Vendors and Outsourcing

a. If a bank decides to use service providers or vendors to provide Electronic banking services, it must exercise appropriate due diligence in evaluating their reputation, financial status, and viability.

b. Banks must ensure that the service providers and vendors can perform as promised and that they are capable of keeping abreast of new or changing technology.

c. When contracting for Electronic banking services, banks must carefully consider how they intend to use third parties to design, implement, and support all or part of their Electronic banking systems.

d. Banks must ensure that adequate controls are in place to monitor performance levels and to swiftly respond to any problem or emergency, by providing specific performance benchmarks to the service provider.

e. Banks when outsourcing, must maintain control through a Service Level Agreement (SLA) over the services and products provided by third parties.

f. When negotiating contracts, bank managements must confirm that responsibilities and accountability are clearly defined for each party.

g. Banks must ensure that they could exercise the control necessary to properly manage the products or services.

h. Control items must include, but not limited to, a bank's ability to perform audits or to obtain from the service provider or vendor independent internal control audits.

i. Banks must establish controls that allow them to confirm third party recovery plans, review their financial condition, and establish data ownership with the third party.

j. Banks must establish their rights, to the extent possible, in the event a third party fails to perform under the contract or fails altogether.

k. Banks must consider the conditions under which they can terminate or change service providers or vendors without incurring substantial liability in the event plans change or performance standards are not met.

l. Banks must ensure that contract specify insurance to be maintained by the service provider.

m. Legal counsel must review the contract to ensure that they are legally enforceable and reasonably protect the bank from risks.

n. Software escrow agreement must be entered into for turnkey e-banking software packages. The agreement must ensure that all relevant program files and documentation are kept current and completed.

o. Where a vendor maintains the e-banking system operated by the bank in-house, the bank must ensure adequate controls over the vendors' access (including remote access) to the banks system to maintain or upgrade software.

p. Activity logs must be maintained to monitor remote vendor access to the systems.

q. Vendor software distribution procedure must be assessed for adequacy and each release accompanied by sufficient documentation.

r. Banks must notify the Regulatory Authorities of applicable service relationships relating to e banking.

2.0 Monetary Policy

a. Electronic money scheme operators must supply the Central Bank with statistical information, about the volume and value of their transactions, based on an agreed format.

b. All categories of electronic money would be treated as part of the deposit liabilities of banks and subject to the application of reserve requirements.

c. The settlement procedure for e-banking transactions must conform to existing regulations. Settlement should be only through clearing banks operating net settlement schemes with NIBSS to CBN in Lagos, and outside Lagos, through the CBN clearinghouses, and other form of clearing and settlement arrangements as may be approved by CBN from time to time.

d. Only licensed deposit taking institutions can issue electronic payment instruments

e. Only institutions that are members of the cheque clearing system in the country are permitted to participate in inter-bank payment systems for e-banking.

f. Issuers of electronic money would be subjected to prudential supervision. In addition to this, international cooperation would be sought to take care of various supervisory issues that emerge from cross-border e-banking activities.

3.0 Legal Issues

a. Banks are obliged not only to establish the identity of their Customers (KYC principle) but also enquire about their integrity and reputation. To this end, accounts should be opened only after proper introduction and physical verification of the identity of the customer.
b. Digital signature should not be relied on solely as evidence in e-banking transactions, as there is presently no legislation on electronic banking in Nigeria
c. There is an obligation on banks to maintain secrecy and confidentiality of customer's accounts. In e-banking scenario, there is the risk of banks not meeting the above obligation. Banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc because of hacking /other technological failures. Banks should, therefore, institute adequate risk control measures to manage such risks.
d. Banks should protect the privacy of the customer's data by ensuring:
    i. that customer's personal data are used for the purpose for which they are compiled.
    ii. consent of the customer must be sought before the Data is used
    iii. data user may request, free of cost for blocking or rectification of inaccurate data or enforce remedy against breach of confidentiality
    iv. processing of children's data must have the consent of the parents and there must be verification via regular mail.
    v. strict criminal and pecuniary sanctions are imposed in the event of default.

e. In e-banking, there is very little scope for the banks to act on stop payment instructions from the customers. Hence, banks should clearly notify the customers the time frame and the circumstances in which any stop-payment instructions could be accepted.
f. While recognizing the rights of consumers under the Nigerian Consumer Protection Council Act, which also apply to consumers in banking services generally, banks engaged in e-banking should endeavor to insure themselves against risks of unauthorized transfers from customers account's, through hacking, denial of services on account of technological failure etc, to adequately insulate themselves from liability to the customers.
g. Agreements reached between providers and users of e-banking products and services should clearly state the responsibilities and liabilities of all parties involved in the transactions.

4.0 Regulatory and Supervisory Issues

4.1 Risk Management: In order to mitigate the risks associated with all e-banking businesses, banks should have in place a comprehensive risk management process that assesses risks, controls risk exposure, and monitors risks. This comprehensive risk management framework should be integrated into the bank's overall risk

management framework. The risk management process should be supported by appropriate oversight by the board of Directors and senior management and carried out by staff with the necessary knowledge and skills to deal with the technical complexities of new e-banking developments. Towards achieving this, banks should:

a. Establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks.
b. Establish a comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking.
c. Ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.
d. Ensure that clear audit trails exist for all e-banking transactions.
e. Develop appropriate incident response plans to manage, contain and minimize problems arising from unexpected events, including internal and external attacks that may hamper the provision of e-banking systems and services.
f. Ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status of the bank prior to entering into e-banking transactions.
g. Provide customers with the option to decline from permitting the bank to share with third party for cross-marketing purposes any information about the customer's personal needs, interests, financial position or banking activity.
h. Ensure that Customer data are not used for purposes beyond which they are specifically allowed or beyond which customers have authorized.

4.2 Introduction of New e-banking / Electronic Products and Service

The existing regulatory framework over banks would be extended to electronic banking. Therefore only banks, which are licensed, supervised and with physical presence in Nigeria, are permitted to offer electronic banking services in Nigerians. Virtual banks or banks that exist only in cyberspace are not allowed.

a. The products / services can only be offered to the following classes of customers
    i. Residents of Nigeria with a verifiable address within the geographic boundary of Nigeria.
    ii. Any person residing physically in Nigeria as a citizen, under a resident permit or other legal residency designation under the Nigerian Immigration Act.
    iii. Any person known herein as a "classified person" who neither meets condition (i) nor (ii) above but is temporarily in Nigeria may utilize e-banking services limited to acceptance services such as ATMs, POS terminals or other acceptance devices deployed by a regulated institution.

b. The e-banking service should be offered in Naira only. Where such a service is to be provided in foreign currency, it should be to only the holders of ordinary domiciliary accounts, and conform with all other foreign exchange regulations.

c. Electronic banking products and services should comply with the Money Laundering Act 1995 as amended and "Know Your Customer" (KYC) rules

d. Banks wishing to provide transactional and/or enhance existing electronic banking services shall submit to the CBN, an application describing the services to be offered/enhanced and how it fits into the bank's overall strategy. This shall be accompanied by a certification signed by its MD/CEO to the effect that the bank has complied with the following minimum pre-conditions:

   i. That an adequate risk management process is in place to assess, control, monitor and respond to potential risks arising from the proposed electronic banking activities;
   ii. A report from an agreed ICT certification agency, confirming that corporate security policy and procedures that address all security issues affecting its electronic banking system, as contained in the Technology and Security guidelines, particularly the following, exist:

      - Authentication
      - Non-repudiation
      - Authorization
      - Integrity
      - Confidentiality

   iii. The system had been tested through appropriate systems testing and user acceptance testing and the test results are satisfactory
   iv. A business continuity planning process has been adopted including a section on electronic banking channels and systems.

e. The following documents would need to accompany the request:

   i. The resolution of the Board of the bank approving the decision to provide the service/products.
   ii. A report on the electronic banking services to be offered or enhanced, the business objectives for such services and the corresponding procedures.
   iii. The detailed features and mode of operating the scheme
   iv. A description or diagram of the configuration of the bank's electronic banking system and its capabilities, showing:

      - How the electronic banking system is linked to other systems or the network infrastructure in the bank;
      - How transaction and data flow through the network;
      - The types of telecommunications channels and remote access capabilities (e.g. direct modem dial-in, internet access, or both);
      - The types of security controls/measures that are installed;
      - A list of software and hardware components indicating the purpose of the software and hardware in the electronic banking infrastructure;

   v. A detailed description of the bank's security policy/security organization including;
      - Definition of responsibilities for designing, implementing, and monitoring information security measures; and
      - Established procedures for evaluating policy compliance, enforcing disciplinary measures and reporting security violations;
   vi. A copy of the draft contract agreement with the technical partners/Software vendors;

vii. A brief description of the contingency and disaster recovery plans for electronic banking facilities and a plan resolve or address problems, such as complaints, errors and intrusions and the availability of back-up facilities;
viii. A copy of the draft maintenance agreements with the software/hardware provider/s;
ix. The schedule of proposed charges/fees
x. The detailed cost implication, which should include 3 years' financial projection.

f. The CBN, through Banking Supervision Department, would appraise the product/service as well as the applicant-bank's overall financial condition, and its compliance with the CBN rules and regulations based on the latest available Returns and Examination Report on the bank.
The CBN would also ensure that the applicant bank's overall financial condition can adequately support its electronic banking activities and that it has complied with certain comprehensive prudential requirements such as, but not limited to, the following:

i. Minimum capital adequacy ratio for consecutive period of 6 months;
ii. Minimum Liquidity ratio for consecutive period of 6 months;\
iii. Satisfactory solvency, liquidity and profitability positions;
iv. Satisfactory CAMEL composite rating
v. Has a sufficient free fund to undertake the required investment in the electronic banking infrastructure (Hardware, Software, Communications etc.)
vi. That all outstanding major exceptions in the latest examination report of the bank have been addressed.

g. Banks with existing electronic banking services but who do not meet the prescribed prudential standards have six (6) months within which to show proof of improved overall financial condition and/or substantial compliance with CBN's prudential requirements, otherwise, their electronic banking activities will be temporarily suspended until such time that the same have been complied with.

h. Banks with existing electronic banking services that have met the prescribed prudential standards, but whose electronic banking services were previously not approved should within (6) months regularise their position by submitting all the required documentation for necessary approval.

This section of the e-banking Guidelines, in so far as it deals with the introduction of new products and services, supercedes the provisions of the circular on the introduction of new products dated 5th April, 2000 in so far as it is inconsistent herewith.

4.3 Reporting Requirements

a. Banks are required to render separate returns on their e-banking activities to appropriate regulatory authorities as prescribed by the CBN from time to time.

b. Cases of frauds and forgeries relating to e-banking should be highlighted in the returns on frauds and forgeries.

4.4 Penalties

4.4.1 Sanctions, in the form of monetary penalties and/or suspension of the specific electronic banking activity (ies) or both, would be imposed on erring banks and/or their officers for failure to:

a. Seek CBN approval before launching, implementing or, enhancing electronic banking services/products, and/or
b. Submit within the prescribed deadline the required information/documents.

4.4.2 Monetary penalties will be imposed, in accordance with relevant sections of CBN Act/BOFIA 1991 as Amended, as follows:

a. A one-time penalty on the officer/s and/or director/s responsible for failure to seek and obtain the prior approval of the CBN and/or non-submission of required information/documents.
b. A daily penalty on the bank for failure to seek prior approval of the CBN and/or for non submission of required information/documents, for the duration of the period of contravention starting from the day the offence was committed up to the time the same was corrected.