CENTRAL BANK OF NIGERIA

REPORT OF THE TECHNICAL COMMITTEE ON ELECTRONIC BANKING

FEBRUARY 2003

REPORT OF
THE TECHNICAL COMMITTEE ON
ELECTRONIC BANKING

February 2003

1. INTRODUCTION 5

1.1 THE ENVIRONMENT 5

1.2 ELECTRONIC BANKING 5
1.2.1 PERSONAL COMPUTER (PC) 6
1.2.2 TELEPHONE 7
1.2.3 AUTOMATED TELLER MACHINES (ATM) 7
1.2.4 INTERNET 7
1.2.5 CARDS 7

1.3 ELECTRONIC PAYMENTS 7

2. ELECTRONIC BANKING RISKS AND CONTROLS 9

2.1 ENVIRONMENT 9

2.2 NATURE AND TYPES OF RISKS ASSOCIATED WITH ELECTRONIC BANKING 10
2.2.1 STRATEGIC RISK 10
2.2.2 OPERATIONAL RISK 10
2.2.3 SECURITY RISK 10
2.2.4 REPUTATIONAL RISK 10
2.2.5 LEGAL RISK 11
2.2.6 MONEY LAUNDERING RISK 11
2.2.7 CROSS BORDER RISKS 11

2.3 ELECTRONIC MONEY 11

2.4 IMPACT OF E BANKING RISKS 12
2.4.1 IMPACT ON FINANCIAL INSTITUTIONS 12
2.4.2 IMPACT ON REGULATORS/SUPERVISORS 13

2.4.3 RISK MITIGANTS 14

3. INFORMATION AND COMMUNICATION TECHNOLOGY 16

3.1 THE ENVIRONMENT 16

3.2 TECHNOLOGIES 17

3.2.1 COMPUTER NETWORKS AND THE INTERNET 17
3.2.2 PROTOCOLS 18
3.2.3 APPLICATION AND SYSTEM SOFTWARE 18
3.2.4 DELIVERY CHANNELS 19

3.3 SECURITY AND PRIVACY ISSUES 24
3.3.1 SECURITY POLICY 24
3.3.2 IDENTIFICATION 25
3.3.3 AUTHENTICATION 25
3.3.4 ACCESS CONTROL 25
3.3.5 DATA CONFIDENTIALITY 26
3.3.6 DATA INTEGRITY 26
3.3.7 NON-REPUDIATION 27
3.3.8 SECURITY AUDIT TRAIL 27
3.3.9 SECURITY LOG 27
3.3.10 LOG OF MESSAGES 27
3.3.11 BACKUP, RECOVERY & BUSINESS CONTINUITY 28

4. MONETARY POLICY IMPLICATIONS 29

4.1 EFFECT OF E-BANKING ON MONETARY POLICY 29
4.1.1 EFFECT ON DEMAND FOR REQUIRED RESERVES 29
4.1.2 EFFECT ON THE SUPPLY OF RESERVES 30
4.1.3 LOSS OF SEIGNIORAGE 30
4.1.4 THE EFFECT ON THE VELOCITY OF MONEY 31

4.1.5 ADEQUACY OF MONETARY POLICY INSTRUMENTS 31

5. LEGAL AND REGULATORY ISSUES 33

5.1 THE ENVIRONMENT 33
5.1.1 FRAUD IN E BANKING 33
5.1.2 MONEY LAUNDERING 33
5.1.3 JURISDICTIONAL IMPEDIMENT 34
5.1.4 ELECTRONICALLY GENERATED EVIDENCE 34

5.2 LEGAL/REGULATORY ISSUES 35
5.2.1 PRIVACY 35
5.2.2 EVIDENCE ACT 35
5.2.3 CONTRACT LAWS 35
5.2.4 CRIMINAL LIABILITY 36
5.2.5 CONSUMER PROTECTION: 36
5.2.6 ELECTRONIC FUNDS TRANSFER (EFT) 38

6. RECOMMENDATIONS **39**

6.1 ELECTRONIC BANKING RISKS **39**

6.2 INFORMATION TECHNOLOGY **42**
6.2.1 INTERNET BANKING 48
6.2.1 VENDORS AND OUTSOURCING 49

6.3 MONETARY AND BANKING POLICY **50**

7. CONCLUSION **52**

6.4 LEGAL AND REGULATORY ISSUES **52**

APPENDICES **54**

APPENDIX 1 **54**
LIST OF MEMBERS -TECHNICAL COMMITTEE ON ELECTRONIC BANKING 54

APPENDIX 2 **55**
QUESTIONNAIRE 55

1. INTRODUCTION

1.1 THE ENVIRONMENT

In Nigeria, and many other countries, banks and financial institutions play an important role in the economy by gathering deposits, repackaging them into a variety of financial products and services for their customers and the public.

Of important consideration here, is the use of Information and Communication Technology to provide the financial products and services for improved efficiency and effectiveness. These continuously affect the risk management, infrastructure provision, monetary policy development and regulatory framework of the financial system.

Advancements in Information and Communication Technology have impacted positively on service delivery in the financial sector of the Nigerian economy. These developments have however not been matched with appropriate legislation/regulation to address the resultant changes in the relationships, responsibilities, liabilities and rights of the parties engaged in electronic banking.

Recognizing the potential for abuse and mismanagement inherent in the financial system, and the negative effect a weak system will have on the economy, the Federal Government and its agencies must be actively engaged in creating an extensive set of laws and regulations to address the inadequacies of the current system.

Also of concern is the potential of digital money to replace fiduciary currency as the predominant payment medium and its ability to flow freely across national borders, raising questions about the effect of e-money on monetary policy.

A central bank's oversight of the financial sector of any economy derives from the fact that it is the sole issuer of currency, and it is through control of money supply that the overall objectives of monetary policy can be realized. Therefore monetary policy objectives should not be constrained by the replacement of fiduciary money with the digital equivalent.

1.2 ELECTRONIC BANKING

Electronic banking may be defined as a means whereby banking business is transacted using automated processes and electronic devices such as personal computers, telephones, fax machines, Internet, card payments and other electronic channels. Some banks practice electronic banking for informational purpose, some

for simple transactions such as checking account balance as well as transmission of information, while others facilitate funds transfer and other financial transactions. Many systems involve a combination of these capabilities.

A survey was conducted in September 2002 to determine the level and types of e-banking activities carried out by banks. The survey showed that 17 banks were offering Internet banking, 24 were offering basic telephone banking, 7 had ATM services, while 13 of the banks indicated that they were offering other forms of e-banking. Twelve (12) of the banks indicated that their websites were hoisted in Nigeria while 22 were hoisted overseas. Fourteen (14) of the websites were information only, 11 were information transfer system while 22 were transactional. 27 of the banks indicated that they had security policies on e- banking while 4 reported that they had none in place. Thirty (30) of the banks reported that they used authentication as a means of security control, 28 used firewalls, 16 cryptography, 8 use digital signature, 14 digital certificate, 18 used Secured Socket Layer (SSL), 15 Public Key Infrastructure (PKI), and 31 used Physical Security.

TABLE 1: Banks engaged in E-Banking in Nigeria

	Internet Facilities	**Transactional**	**Information Only**	**Information Transfer**	**Telephony Banking**	**Others**	**ATM**	**Security Policy In Place**
Banks	39	22	14	11	24	13	7	27

Source: BSD, CBN

The following are some of the electronic services that have been introduced by the banks:

1.2.1 PERSONAL COMPUTER (PC) BANKING

PC banking refers to the use of computer hardware, software and telecommunications to enable retail customers' access to both specific account and general information on bank products and services through a personal computer.

1.2.2 TELEPHONE BANKING

Telephone links are used in electronic banking for direct connection either as private networks such as direct dial-in using leased or dedicated telephone lines or public networks.

1.2.3 AUTOMATED TELLER MACHINES (ATM)

ATMs enable cardholders to withdraw cash, make deposits or transfer funds between accounts. To use the ATM, a Smartcard is inserted and a PIN (Personal Identification number) is entered to give the customer access to cash all day long.

1.2.4 INTERNET BANKING

The Internet enables electronic banking through connections to the bank for a wide variety of services.

1.2.5 CARDS

Cards are a key tool for electronic banking, providing authentication and access to banking services. Most common in Nigeria are Smart cards containing one or more integrated circuit chips supporting multiple applications, thereby facilitating access to funds in the cardholders account on the basis of information communicated electronically.

1.3 ELECTRONIC PAYMENTS

The most common channel of electronic payments delivery in Nigeria is the smart card. The full range of electronic transactional banking, such as funds transfer via the Internet, has experienced limited growth, as there are very limited operational online (web based) payment systems in country.

Due to the lack of an appropriate online payment system, online retailers in Nigeria cannot sell and accept payments for goods on the internet. The few existing transactional web sites accept only international cards such as Visa and MasterCard.

There is a growing use of smart cards such as Valucard and SmartPay Card in the payment space. Available data indicate that between 2000 and 2002, the number of smart cards issued quadrupled, while the value of transactions grew by more that 250 percent (See Table 2). Similarly the number of ATMs has increased from a modest 3 in 2000 to 68 in 2002.

Table 2: Growth of E-Banking / Payments in Nigeria

	2000	**2001**	**2002**
Point of Sale (POS) Machines/Locations	1,027	1,660	1,799
Value of Transactions (=N='m)	3,201	6,945	8,939
No. Of Cards Issued	35,693	66,112	134,054
No of ATMS	3	43	68

Source: BSD, CBN

Mobile phones are increasingly being used for financial services, leveraging connectivity to link customers. Banks are enabling the customer to conduct most banking services from inquiry to initiating transactions.

ATM growth has increased fourfold over the past three years, and is expected to grow from the current 68 units to over 1000 units by 2004.

International Cards such as Visa card have seen limited use as a result of the lack of supporting telecommunications infrastructure. However this situation is improving following the liberalization of the telecommunications sector.

2. ELECTRONIC BANKING RISKS AND CONTROLS

2.1 ENVIRONMENT

Electronic banking systems primarily expose banks to transaction, strategic, reputation, and compliance risks, but may expose a bank to other risks as well. For example, Electronic-banking systems may present credit risk if a bank offers lending services over the Internet. Requirements such as "Know your customer" may require the use of different identification, authentication, and transaction verification methods than those used with traditional delivery channels. Liquidity, interest rate, market, price, and foreign exchange risks may also result from poor data integrity or unreliable systems. The Regulatory/Supervisory Authorities expect banks to carefully consider the full range of these and other issues and the potential risks that they may pose in deciding whether to adopt an electronic banking product or to renovate an existing one.

Electronic banking risks should be managed as part of a bank's overall risk management process. Banks should use a rigorous analytic process to identify, measure, monitor, and control risks. The quantity of risk assumed should be consistent with the bank's overall risk tolerance and must not exceed the bank's ability to manage and control its risks. Management and bank staff are expected to have the knowledge and skills necessary to understand and effectively manage their Electronic banking-related risks. Examiners will evaluate Electronic-banking risks by reviewing technology plans, policies, controls, monitoring techniques, and relevant compliance issues. In addition, the Regulator may evaluate system performance and the effectiveness of specific controls.

Regardless of how a system is developed or operated, the regulator's expectation is for banks to effectively manage their Electronic banking risks. Controls should take into account the level of risk posed to the institution and should be adopted by the party in the best position to control the risks. In some instances, that party may be an outside vendor or service provider. In practice, the controls necessary to effectively manage risk will differ depending on the degree of risk posed and how the Electronic banking system is designed and operated.

2.2 NATURE AND TYPES OF RISKS ASSOCIATED WITH ELECTRONIC BANKING

The risks associated with e-banking and e-money activities as per Basle Committee's categorization of risks include: Strategic Risk, Operational Risk, Security Risk, Reputational Risk, Legal Risk, Money Laundering Risk, Cross Border Risks and Other Risks. These risks are briefly discussed below:

2.2.1 STRATEGIC RISK

Strategic risks are those risks associated with board and management decisions. This risk could arise as a result of weak, shallow, corrupt or not well thought out projects planning, timing and implementation. However, the degree of this risk depends upon how well the institution has addressed the various issues related to development of a business plan, availability of sufficient resources to support this plan, credibility of the vendor (if outsourced) and level of the technology used in comparison to the available technology etc.

2.2.2 OPERATIONAL RISK

Operational risks take the form of inaccurate processing of transactions, non-enforceability of contracts, compromises in data integrity, data privacy and confidentiality. Also, inadequacies in technology, human factors such as negligence by customers and employees, fraudulent activity of employees and crackers/hackers can become potential source of operational risk.

2.2.3 SECURITY RISK

Security risk refers to the unauthorized access or intrusion to a bank's information systems and transactions. Attackers could be hackers, unscrupulous vendors, disgruntled employees or even pure thrill seekers. Also, in a networked environment the security intrusion is often limited to the weakest link.

2.2.4 REPUTATIONAL RISK

Reputational risk is the risk of getting significant negative public opinion, which may result in a critical loss of funding or customers. These are risks arising from banks' or

third parties actions resulting to a major loss of the public confidence in the banks' ability to perform critical functions or impair bank-customer relationship.

These actions vary from system or product not working to the expectations of the customers, significant system deficiencies, significant security breach, inadequate information to customers about product use and problem resolution procedures, significant problems with communication networks that impair customers' access to their funds or account information especially if there are no easy alternative means of account access.

2.2.5 LEGAL RISK

Legal risk results from violation of, or non-conformance with laws, rules, regulations, or prescribed practices, or when the legal rights and obligations of parties to a transaction are not well established in the course of delivery of banking services and products via electronic channels.

2.2.6 MONEY LAUNDERING RISK

This is a risk that financial institutions are exposed to when their systems are used in moving criminal funds.

2.2.7 CROSS BORDER RISKS

Cross border risks are risks that banks are exposed to in the course of their international transactions arising from differences in legal/regulatory and jurisdictional ambiguities with respect to the responsibilities of different national authorities. These risks are associated with non-compliance of different national laws and regulations, including consumer protection laws, record-keeping and reporting requirements, privacy rules and money laundering laws.

By the nature of cross border risk apart from the legal risk, a bank could also be exposed to other risks like the operational, credit risk and market risk as a result of geographical and market expansion beyond the national borders which make monitoring more difficult.

2.3 ELECTRONIC MONEY

Another facility of e-banking is electronic money. Electronic money is an electronic store of monetary value on a technical device (smart cards) that may be widely used for making payments to undertakings other than the issuer without necessarily involving bank accounts in the transaction, but acting as a prepaid instrument. Risks that are also associated with electronic money are broadly divided into two.

1. **Quantifiable Risks** comprising of credit, liquidity, interest rate, foreign exchange and equity prices.

2. **Non-Quantifiable Risks** comprising of strategic, operational, compliance, reputational and legal risks, which have already been explained under electronic banking.

2.4 IMPACT OF E BANKING RISKS

While the basic types of risks generated by electronic banking and electronic money are not new, the magnitude of their impact on banks and merchants may be new for them and regulators/supervisors. The impact of the risks these banks/merchants face are embedded in the types of risks associated with e-banking and e-money. Some of them are discussed and examined below:

2.4.1 IMPACT ON FINANCIAL INSTITUTIONS

Financial institutions are often faced with system redundancy due to rapid technological changes resulting to excessive costs particularly if an institution wants to be a technological pioneer just as in the case of an overly cautious technology follower which may find itself unable to adequately position itself in a saturated market or a market that is consolidating rapidly.

Operational/Security Risks

These could lead to financial and capital losses due to inaccurate processing of transactions, non-enforceability of contracts, compromises in data integrity, data privacy and confidentiality, unauthorized access/intrusion to Financial Institutions systems and transactions. Others include technological inadequacies or problems of integration, outsourcing, Internet and third party services. Apart from financial losses, financial institutions also face the problems of loss of data, theft or tampering with customer information, disabling of a significant portion of Financial Institution's internal computer systems due to the activities of hackers.

Reputational Risks

Financial Institutions could face or experience problems of negative public opinion which result in critical loss of fund or customers arising from Financial Institutions or third party actions which could result to loss of public confidence in the Financial Institutions' ability to perform critical functions or impair Financial Institution-customer relationship. In the same vein, it may have a bandwagon effect on other Financial Institutions that are providing similar services.

Legal Risks

Financial institutions could face transactional disputes, unwanted suits or other regulatory sanctions due to inadequate information to customer about his rights and obligations to enable him take proper precautions in using Internet banking products or services.

Also e-banking cuts across national boundaries bringing uncertainties and ambiguity about legal requirements. Financial Institutions are exposed to legal risks associated with non-compliance of different national laws and regulations, including consumer protection laws, record-keeping and reporting requirements, privacy rules and money laundering laws.

As Internet banking transactions are conducted remotely, banks could also be faced with legal sanctions for non-compliance with "know your customer" laws due to difficulties in applying traditional methods in detecting and preventing undesirable criminal activities.

Cross Border Transaction Risk

This accentuates credit risk, since it is difficult to appraise an application for a loan from a customer in another country compared to a customer from a familiar customer base. Financial Institutions accepting foreign currencies in payment for electronic money may be subjected to market risk because of movements in foreign exchange rates.

2.4.2 IMPACT ON REGULATORS/SUPERVISORS

As the preceding discussion indicates, the basic types of risks associated with e-banking are not new. However, the specific ways in which these risks arise, as well as, the potential magnitude and speed of impact on banks, may be new for bank

management and supervisors alike. In addition, while assessing risk should be dynamic, the rapid pace of technological innovation supporting e-banking, the increased degree of systems outsourcing and the reliance of some products/services on the use of open networks such as the Internet, intensifies the need for a rigorous and ongoing risk management process.

It is therefore essential for bank supervisors to recognize their own critical need for appropriate technology knowledge and skills to ensure that they understand the risks and challenges arising from the development of the e-banking delivery channels. Towards achieving this, enhanced technical training is essential for the supervisory staff and if necessary, to be complemented by appropriate attachment programs with other overseas regulatory/supervisory bodies.

2.4.3 RISK MITIGANTS

To reduce strategic risk, financial institutions management should conduct proper survey, consult experts from various fields, establish achievable goals and monitor performance. Also they will need to analyze the availability and cost of additional resources, provision of adequate supporting staff, proper training of staff and adequate insurance coverage. Due diligence needs to be observed in selection of vendors, audit of their performance and establishing alternative arrangements for possible inability of a vendor to fulfill its obligation. Besides this, periodic evaluations of new technologies and appropriate consideration for the costs of technological up gradation are required.

To limit operational risk, banking organizations should use an integrated enterprise-wide architecture and technology infrastructure that can facilitate interoperability, ensure the security, integrity and availability of data and support the management of relationships with third-party service providers.

Data privacy and confidentiality issues must be given serious attention by the management to address security risk. Weak network links must also be properly protected through the use of firewalls, encryption, authentication, etc.

Possible measures to avoid reputational risk are to test the system before implementation. Provision must also be made for back-up facilities, contingency plans including plans to address customer problems during system disruptions, virus checking devices and the deployment of ethical hackers for plugging the loopholes and other security measures.

Customers must be adequately informed about their rights and obligations in the use of e-banking products by the issuers and validity of agreements must be properly addressed to avoid or minimize legal risks.

To avoid money laundering risks, banks need to design proper customer identification and screening techniques, develop audit trails, and conduct periodic compliance reviews, frame policies and procedures to spot and report suspicious activities in electronic /Internet transactions.

Proper evaluation of credit worthiness of a customer and audit of lending process are a must to avoid credit risks.

3. INFORMATION AND COMMUNICATION TECHNOLOGY

3.1 THE ENVIRONMENT

Electronics have provided a new and inexpensive channel for banks to reach out to their customers. It allows customers to access banks' facilities round the clock, seven days a week. It also allows customers to access these facilities from remote sites, home etc. However, all these capabilities come with a price. The highly unregulated Electronic Banking provides a less than secure environment for the banks to interface. The diversity in computer hardware, communication and software technologies used by the banks vastly increases the challenges facing the online bankers. In this section, an effort has been made to give an overview of the technologies commonly used in electronic banking. An attempt has also been made to describe concepts, techniques and technologies related to privacy and security - including physical security. The banks planning to offer electronic banking should have explicit policies on security. An outline for a possible framework for security policy and planning is included in this report.

Banks have over the years expanded their technology capabilities at significant costs. Investments have been aborted in midstream in many cases due to obsolescence of technology or poor planning. Of concern are the increasing levels of investment in technology by banks sometimes running into hundreds of millions of naira, which are not currently being monitored. For example, when a single bank proposes to deploy large number of ATMs, for significant capital outlay, the regulatory authorities should naturally be concerned and need to determine if banks are limiting their investments, which are capital in nature, to the free funds available to such banks (shareholders funds less investments in fixed assets and equities). The Committee therefore proposes that banks should obtain the approval of the Central Bank for new investments in technology where such investments exceed 10% of free funds. The thresh hold of 10% is meant to prevent the CBN being inundated with requests for approval of purchases that are not material in value.

3.2 TECHNOLOGIES

3.2.1 COMPUTER NETWORKS AND THE INTERNET

The purpose of computer networking is sharing of computing resources and data across the whole organization and the outside world. Computer Networks can be primarily divided into two categories based on speed of data transfers and geographical reach. A Local area network (LAN) connects many servers and workstations within a small geographical area, such as a floor or a building. The Wide Area Network (WAN), on the other hand, is designed to carry data over great distances and is generally point-to-point. The different topologies, technologies and data communication protocols have different implications on safety and security of services. Banks need to ensure that their LAN's are adequately protected from users outside the system as well as unauthorized access within the network. In the case of WAN's, banks need to ensure that, as data travels across greater distances, adequate measures are in place to protect the data while in transit. This is most critical as banks begin to deploy wireless LANS and Satellite based shared hubs. In either case, banks must ensure that their networks provide adequate security for the data being transmitted while enabling access to the data by authorized persons.

Specifically networks used for transmission of financial data most be certified to meet the requirements specified for data confidentiality and integrity.

Banks should be required to deploy a proxy type firewall to prevent a direct connection between the banks' back-end systems and the Internet. Banks should also be required to ensure that the implementation of the firewalls address the security concerns for which they are deployed. 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.

External devices such as ATMs, PC's at remote branches, kiosks, etc. that are permanently connected to the bank's network and pass through the firewall must at the minimum be authenticated via Media Access Control (MAC) address in addition to other methods such as IP Addresses.

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

3.2.2 PROTOCOLS

The data transmission protocol suite used for the Internet is known as the Transmission Control Protocol/Internet Protocol (TCP/IP). The Internet is primarily a network of networks. The networks in a particular geographical area are connected into a large regional network. With the popularity of the web, organizations find it beneficial to provide access to their services through the Internet to its employees and the public. The web-based applications provide flexible access from anywhere using the familiar browsers that support graphics and multimedia. The solutions are also scalable and easy to extend. 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 should be required to ensure that unnecessary services and ports are disabled.

3.2.3 APPLICATION AND SYSTEM SOFTWARE

Electronic banking applications run on diverse platforms, operating systems and use different architectures. The product may 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 DBMS package. Moreover, the product may run on computer systems of various types ranging from PCs, open systems, to proprietary main frames. These products allow different levels of access to the customers and different range of facilities. However, banks must be mindful of the limitations of communications for server/client-based architecture in an environment where multiple servers may be more appropriate.

In addition banks must clearly understand the need for their banking applications to interface with a number of external sources. Banks must ensure that applications deployed can support these internal interfaces or provide the option to incorporate these interfaces at a later date. Critical is how banks will 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.

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

The bank's Information Systems infrastructure must be properly physically secured. Banks may be required to develop policies setting out minimum standards of physical security.

Banking applications run by the bank should be required to have proper record keeping facilities for legal purposes. It may be necessary to keep all received and sent messages both in 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.) Such information must be stored in conformity with existing legal requirements.

Banks should be required to identify an ICT compliance officer whose responsibilities should include compliance with standards contained in the guidelines ICT policy.

3.2.4 DELIVERY CHANNELS

Electronic delivery channels available to banks are numerous and require that banks understand the inherent capabilities and limitations of each channel. Channels include, the internet, Cards, Mobile devices and PDA's, ATM's Telephones, personal computers etc.

Mobile Telephony

Mobile phones are increasingly being used for financial services leveraging connectivity to link customers. Banks are enabling the customer to conduct most banking services from inquiry to initiating transactions. As indicated in these guidelines, the primary concern of the regulatory authorities will be to;

1. Secure the data transmitted and
2. Maintain an audit trail of individual transactions.

As a result, networks used for transmission of financial data must be demonstrated to meet the requirements specified for data confidentiality, integrity and non-repudiation. In addition an audit trail of individual transactions must be kept.

Settlement of e-payments transactions delivered through mobile telephony should be done through the banking system.

Automatic Teller Machines (ATMs)

ATM growth has increased fourfold over the past three years, and is expected to grow from the current 68 units to over 1000 units by 2004, as a result the regulatory authorities feel a compelling need to address issues relative to this channel. Since some ATMs may be offsite or at the bank branch, networks used for transmission of ATM transactions must be demonstrated to meet the requirements specified for data confidentiality and integrity. In view of the demonstrated weaknesses in the magnetic stripe technology, there is the need for banks to standardise to the chip (smart card) technology. A time frame of 5 years is considered appropriate. For banks that have not deployed ATMs, the expectation is for the banks to deploy chip based ATMs. 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. Banks should be advised to note that the regulatory authorities will consider fraud liability as a result of card scheming, counterfeit cards to be responsibility of the bank.

Banks should be encouraged to join shared ATM networks and should be required to display clearly on the ATM machines the Acceptance Mark of the cards usable on the machine.

All ATMs not located in 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 the ATM is in operation and a mirror must be placed around the ATM to enable the individual using the ATM to determine the locations of persons in their immediate vicinity. Most importantly the ATM 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.

ATMs may not be placed outside buildings unless such ATM is bolted to the floor and surrounded by structures to prevent its removal. Additional precaution must be taken to ensure that any network connectivity from the ATM to the bank or switch must be protected to prevent the connection of other devices to the network point.

Organisations other than financial institutions may own ATMs, however such organisations must enter into an agreement with a financial institution (Processing bank) for the processing of the transactions at the ATM. The funding (provision of cash in the ATM) and operation of the ATM should be the sole responsibility of the bank. If an ATM is owned by a non bank organisation, processing banks must ensure

that the card reader, as well as other devices that capture/store information on the ATM, do not expose to the owner of the ATM, information such as the PIN number or other information that is confidential.

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

ATMs at bank branches should be situated in such a manner as to permit access to the ATM 24 hours a day, 7 days a week. Banks must ensure that when the ATM is accessed at hours other than when the bank is opened, that access is granted to the ATM by a security staff of the bank or by the use of a card thereby limiting access to non-ATM customers. This is to ensure the safety of those using the ATM at off banking hours.

Cameras used to record the activity of a customer at the ATM must not be able to record the keystrokes of such customer. A telephone should be available to the customer to report incident at the ATM including inability to draw cash or other failures that take place. Such telephone line must be manned at all times the ATM is operational

Point of Sale (POS) Devices

Providers that place 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.

Private companies may deploy Point of Sale terminals, however such companies should be required to sign agreements with banks that are responsible to the merchant for transactions done on the terminals.

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 that is hereafter classified as confidential. The device should not have the capability of printing a customers PIN number for any reason whatsoever.

Providers of point of sale devices should be encouraged to accept cards from other schemes.

International Card Schemes

Banks should be encouraged to issue international cards (such as Visa/MasterCard etc.) to their customers. Such cards however should only be used outside Nigeria and payment on the cards should only be done through an ordinary domiciliary account or other account that may be permitted by the Regulatory Authorities. Banks may acquire international cards for which the merchant receives value in Naira at the applicable rate at the Central Bank for the currency on the date of settlement.

3.2.4 ELECTRONIC BILL PRESENTMENT AND PAYMENT (EBPP)

Settlement should be done through the banking system. Third party (none bank) providers must first enter into agreement with financial institutions that will act as the settlement organization.

3.2.4 SWITCHES

As switches connect consumers to their bank accounts to authorize transactions, only banks or a consortium of banks or agents for banks or banking consortium or any other company as approved by the CBN, can act as a switching company. 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 the 3rd party service provider agreement. Third parties or service providers must meet the guidelines as described under “Guidelines for Vendors and Outsourcing”.

Switching companies should be required to preserve records of transactions for a minimum of five (5) years for audit and investigation purposes. Banks whose transactions are switched should be required to retain records of the transaction for a minimum of the five (5) years. Records should be retained in an easily retrievable format.

3.2.5 CARD SCHEMES

Cards should only be issued by deposit taking institutions duly licensed by the Central Bank of Nigeria, however where cards are used in a closed environment, such as telephone cards used by a telephone company for it's 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 outside the closed group.

Banks should be encouraged to 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. This can be achieved by having the Central Bank issue the first six numbers for each card issuing organization, followed by a card numbering sequence chosen by the bank. 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 should consider using a sixteen (16) digit numbering sequence. The Central Bank of Nigeria should 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.

3.2.6 ELECTRONIC FUNDS TRANSFER (EFT)

Only authorized financial institutions should undertake EFT transactions. Companies that offer switching services should be licensed as EFT Messaging Companies. Operators must ensure a safe and sound EFT network-switching environment, which with adequate internal controls, minimize errors, discourage fraud and provide an adequate audit trail.

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 should be notified of fees charged as well as changes to the fees charged for services.

Management should ensure the existence of written and approved policies and procedures covering personnel, security controls, operations and disaster recovery that must be enforced.

EFT Operators must conform to guidelines for security and privacy policies established by the Central Bank of Nigeria.

3.3 SECURITY AND PRIVACY ISSUES

3.3.1 SECURITY POLICY

Banks should have in place a security policy duly approved by the bank's Board.

The information security policy is the systemization of approaches and policies related to the formulation of information security measures to be employed within the organization to assure security of information and information systems owned by it. The security policy should address the following issues:

1. Basic approach to information security measures.
2. The information and information systems that must be protected, and the reasons for such protection.
3. Priorities of information and information systems that must be protected.
4. Involvement and responsibility of management and establishment of an information security coordination division.
5. Checks by legal department and compliance with laws / regulations.
6. The use of outside consultants.
7. Identification of information security risks and their management.
8. 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).
9. Decision making process of carrying out information security measures.
10. Procedures for revising information security measures.
11. Responsibilities of each officer and employee and the rules (disciplinary action etc) to be applied in each case.
12. Auditing of the compliance to the security policy.
13. User awareness and training regarding information security.
14. Business Continuity Plans.
15. Procedures for periodic review of the policy and security measures.
16. Procedures for change and configuration management covering all facilities.

The top management of the bank must express a commitment to security by manifestly approving and supporting formal security policy, awareness and training. Security awareness will teach people not to disclose sensitive information such as password file names. Security guidelines, policies and procedures affect the entire organization and as such, should have the support and suggestions of end users, executive management, and security administration, Information and Communications Technology (ICT) personnel and legal counsel.

3.3.2 IDENTIFICATION

All users and critical devices on networks used for e-banking have 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) All identities should be aged and renewed on expiry.

3.3.3 AUTHENTICATION

A minimum of two-factor authentication process should be 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.

Authentication is the process of verifying claimed identity of an individual user, machine, software component or any other entity. For example, an IP Address identifies a computer system on the Internet, much like a phone number identifies a telephone. It may be to ensure that unauthorized users do not enter, or for verifying the sources from where the data are received. It is important because it ensures authorization and accountability. Authorization means control over the activity of user, whereas accountability allows us to trace uniquely the action to a specific user. Authentication can be based on password or network address or on cryptographic techniques.

3.3.4 ACCESS CONTROL

Banks should introduce logical access controls over ICT infrastructure deployed.

Access controls are mechanisms to control the access to the system and its facilities by a given user up to the extent necessary to perform his job function. It provides for the protection of the system resources against unauthorized access. An access control mechanism uses the authenticated identities of principals and the information about these principals to determine and enforce access rights. It goes hand in hand with authentication. In establishing a link between a bank's internal network and the Internet, a number of additional access points into the internal operational system might be created. In this situation, unauthorized access attempts might be initiated

from anywhere. Unauthorized access causes destruction, alterations, theft of data or funds, compromising data confidentiality, denial of service etc. Access control may be of discretionary and mandatory types.

Controls instituted by banks should be tested through periodic Penetration Testing, which should include but should not be limited to:

1. Password guessing and cracking
2. Search for back door traps in programs.
3. Attempts to overload the system using Ddos (Distributed Denial of Service & DoS (Denial of Service) attacks.
4. Check if commonly known vulnerabilities in the software still exist.

Banks may for the purpose of such Penetration Testing employ external experts.

3.3.5 DATA CONFIDENTIALITY

The concept of providing for protection of data from unauthorized disclosure is called data confidentiality. Due to the open nature of Internet, unless otherwise protected, all data transfer can be monitored or read by others. Although it is difficult to monitor a transmission at random, because of numerous paths available, special programs such as "Sniffers", set up at an opportune location like Web server, can collect vital information. This may include credit card number, deposits, loans or password etc. Confidentiality extends beyond data transfer and includes any connected data storage system including network storage systems. Password and other access control methods help in ensuring data confidentiality.

3.3.6 DATA INTEGRITY

It ensures that information cannot be modified in unexpected way. Loss of data integrity could result from human error, intentional tampering, or even catastrophic events. Failure to protect the correctness of data may render data useless, or worse, dangerous. Efforts must be made to ensure the accuracy and soundness of data at all times. Access control, encryption and digital signatures are the methods to ensure data integrity.

3.3.7 NON-REPUDIATION

Non-Repudiation involves creating proof of the origin or delivery of data to protect the sender against false denial by the recipient that data has been received or to protect the recipient against false denial by the sender that the data has been sent. To ensure that a transaction is enforceable, steps must be taken to prohibit parties from disputing the validity of, or refusing to acknowledge, legitimate communication or transaction.

3.3.8 SECURITY AUDIT TRAIL

A security audit refers to an independent review and examination of system's records and activities, in order to test for adequacy of system controls. It ensures compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in the control, policy and procedures. Audit Trail refers to data generated by the system, which facilitates a security audit at a future date.

3.3.9 SECURITY LOG

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.

3.3.10 LOG OF MESSAGES

The banking applications run by the banks should have proper record keeping facilities for legal purposes. It may be necessary to keep all received and sent messages both in 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.)

3.3.11 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.

Back-up of data, documentation and software is an important function of the administrators. Both data and software should be backed up periodically. The frequency of back up should depend 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. 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. 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.

4. MONETARY POLICY IMPLICATIONS

4.1 EFFECT OF E-BANKING ON MONETARY POLICY

The potential of digital money replacing currency as the predominant means of paying for retail goods and its ability to flow freely across international borders has raised conflicting questions about the ultimate effect of e-money on monetary policy. This is because central banks' command over the financial resources of any economy derives from the fact that they are the sole issuers of currency, and it is through control of money supply that the overall objectives of monetary policy can be realized. Therefore, in a situation where it is potentially possible for digital money to replace fiduciary money, serious monetary policy implications would emerge. Some of the opposing tendencies on the possibilities are as follows:

- Protagonists believe that central banks would lose control over the monetary aggregates, and even worse, that digital money could alter foreign exchange rates, disturb money supplies, and encourage an overall financial crisis.

- Opposing views hold that digital money is no different from all other forms of money that exist today; consequently the monetary policy implications of digital money are negligible.

A more profound concern is the assumption that maintenance of price stability, the ultimate goal of central banks could be jeopardized if the introduction of electronic money product or e-money, nullifies the relationship between issuance of money by the central bank and the price level.

Some of the issues that are likely to confront the CBN as the scope for e-money and e-banking expands are as follows:

4.1.1 EFFECT ON DEMAND FOR REQUIRED RESERVES

Banks hold a percentage of their deposit liabilities in reserve accounts at the Central Bank. Liquidity management, the major monetary operating framework of central banks is hinged on the need to absorb the liquidity that is in excess of what is necessary for price stability and non-inflationary growth. If the use of electronic money becomes more widespread, and consumers hold more and more of their liquid assets in electronic money form, currency in circulation should go down proportionately. When more monetary assets are intermediated by the formal

financial system, the scope for efficiency in the transmission of monetary policy is enhanced.

However, a key issue that could help or hinder the financial intermediation is whether or not digital money is "reservable" in the sense that it is subject to required reserves provision. If unlike other deposit liabilities of banks, electronic money is not subject to mandatory reserve requirements, the scope for additional creation of credit by banks, and the tendency to develop innovative ways of "reserve avoidance" would increase. Therefore the positive effect of reduced currency in circulation may be countermanded by the tendency for additional credit creation by banks.

4.1.2 EFFECT ON THE SUPPLY OF RESERVES

Central Banks liabilities are held in currency. In the event that the substitution in favour of digital money becomes widespread, as noted in the foregoing, currency in circulation would shrink, reducing the total monetary liabilities of the Central Bank. Shrinking monetary base severely constrains the ability of the Central Bank to undertake reserve absorbing monetary operations such as Open Market Operations, which are essential for the achievement of monetary policy objectives. This concern has been raised by the BIS (1996):

"Since cash is a large or the largest component of central bank liabilities in most countries, a very extensive spread of e-money could shrink central bank balance sheets significantly. The issue is at what point this shrinkage might begin to adversely affect monetary policy implementation. The relatively modest size of open market operations on normal days suggests that a relatively small balance sheet might be sufficient. However, special circumstances could arise in which the central bank might not be able to implement reserve-absorbing operations on a large enough scale (for example, to sterilize the effects of large purchases in the foreign exchange markets) because it lacked sufficient assets on its balance sheet".

4.1.3 LOSS OF SEIGNIORAGE

The reduction in cash based transactions implies that the demand for currency would be substantially reduced. If this is the case, the revenue that accrues to the CBN from printing money (seignorage) goes down proportionately. Since the Central Bank would not raise high-powered money in response to falling seignorage revenue, the effect of the loss would most likely reflect in the operating surplus transferred to the government, which would go down, creating a shortfall (deficit) in government revenue.

4.1.4 THE EFFECT ON THE VELOCITY OF MONEY

The basic assumption underlying the Central Bank's monetary programme is that there is a stable velocity of money. The assumption of stable velocity forms the bedrock of the forecast of target levels of monetary aggregates. In the event of increased substitution in favour of digital money, velocity, whose stability is hinged on the presence of stable demand for currency and deposits in certain proportions may move erratically, and affect the achievement of set targets for monetary aggregates.

Considering the aforesaid, it is clear that monetary policy would be affected by increased holdings of electronic money, and this calls for a re-examination of the adequacy of existing monetary policy instruments.

4.1.5 ADEQUACY OF MONETARY POLICY INSTRUMENTS

In the light of the aforementioned discussions, monetary policy instruments such as Open Market Operations (OMO) and cash reserve requirements may be limited in their efficiency in the face of expanded usage of electronic money, as they may not be able to capture the nuances of e-money as efficiently as required. This might necessitate the development of more robust instruments for the achievement of monetary policy objectives. It has been suggested that since most of the changes arising from the substituting of cash for electronic money affects money narrowly defined (M1), the Central Bank can take certain measures to prevent potential changes in M1. Some of these are:

- Limit the proliferation of digital money products to prevent the replacement of central bank currency.
- Issue digital money products and treat digital money balances in the same way as central bank currency.[1]
- Apply high reserve requirements on digital money balances.
- Absorb – sterilize – the excess liquidity created by appropriate monetary operations.

Though these recommendations are practicable, in reality, they are beset with certain drawbacks. For example, legal restrictions to prevent the proliferation of digital

[1] The Central Bank of Finland, for example is developing a cash card system through a subsidiary company.

money products will be difficult to justify, especially in light of efforts to deregulate and improve the efficiency of the financial sector.

Secondly, digital money products offer substantial cost saving compared with paper cheques, and measures that prevent development of digital money product will result in a competitive disadvantage. Nations that will develop these products will thereby take a lead in a crucial technological sector. In addition, digital money easily crosses international borders and it will be difficult to control foreign digital money products that could eventually emerge as a medium of exchange in the home country.

The drawback of the first three measures is that they may reduce the private sector's incentive to invest in the development of digital money products, which could be costly to the economy in the long run. The possibility open to the Central Banks is to fine-tune its operating procedures and instruments so as to achieve the desirable growth in money, rather than stifle the development of electronic money.

5. LEGAL AND REGULATORY ISSUES

5.1 THE ENVIRONMENT

Despite the phenomenal increase in e-banking activities in Nigeria today, it is unfortunate that this trend has not been matched with commensurate development in the legal framework for the practice of e- banking. In Nigeria, reliance is being placed on existing legislations, regulations, rules and codes of professional ethics evolved in relation to paper-based transactions to deal with electronic banking issues.

It is therefore necessary to critically examine the legal issues involved in e- banking against the existing legal framework with a view to making necessary recommendations.

5.1.1 FRAUD IN E BANKING

One very serious concern in e-banking is the high exposure of the system to fraudsters, hackers and other criminally minded persons who could access, retrieve and utilize confidential information from the system if appropriate security measures are not put in place to checkmate unauthorized intrusion into the system. A story was told a few years ago of a graduate of Chemistry of St. Petersburg Institute of Technology Russia, who was alleged to have transferred well over $11 million from Citibank's Computer database in New York to accounts in Israel, San Francisco and Finland.

This incident, among others, has brought to the fore the risk of fraud prevalent in e banking.

5.1.2 MONEY LAUNDERING

Developments in information technology particularly the growing use of the internet, has now made it possible to conduct a wide range of commercial activities electronically.

The growth of electronic commerce has increased the concern about the use of electronic medium to launder money. Happily enough, Nigeria has a Money Laundering Law in place and all that is required at the moment is the enlargement of its scope to cover the laundering of money derived from other criminal activities. Secondly, emphasis must be placed on the preparedness of our law - enforcement agencies to enforce the law. Equally, banks need to design proper customer

identification and screening techniques, develop audit trails, conduct compliance reviews formulate policies and procedures to spot and report suspicious activities in electronic/internet transactions.

5.1.3 JURISDICTIONAL IMPEDIMENT

E-banking transaction transcends the national borders. The issue of the applicable law becomes rife in electronic banking transaction involving money transfers from jurisdictions outside Nigeria. The question is, in the event of any dispute, which law will apply? Over the years, the courts have adopted certain guiding principles where the issue of jurisdiction arises in a dispute. In such a situation, the courts have had recourse to the following:

1. Statutory provision (if any);

2. Contractual provision (if any);

3. The law of the jurisdiction closely connected with the contract either in terms of where the contract was made or where it is expected to be executed or where the parties are domiciled.

5.1.4 ELECTRONICALLY GENERATED EVIDENCE

Most transactions, whether electronic or manual, have the propensity to generate or lead to dispute. The resolution of such dispute may take the form of one of the following medium of dispute resolution: negotiation, arbitration or litigation. To resolve any dispute utilizing any of the identified medium requires the indispensable use of evidence.

Evidence in electronic banking transactions are essentially electronically generated documents, from either the hard disk or the floppy disk. Such electronically generated evidence qualifies to be classified as secondary evidence as provided in section 93 of the Nigerian Evidence Act. For such secondary evidence to be admissible certain conditions set out in section 94 of the Evidence Act must be satisfied i.e., when the original is immovable, lost or cannot be produced.

It has further been argued that the Computer print-out cannot be regarded as a copy of the original since the original is in code (Derryck Lowery (2001).

5.2 LEGAL/REGULATORY ISSUES

5.2.1 PRIVACY

Under Section 37 of the 1999 constitution it is constitutionally guaranteed. It is recommended however, that in the penal provision of the proposed e-banking legislation, stiff penalties should be imposed on hackers and unauthorized intruders into the system to act as deterrent to others.

The banking regulatory authorities should be able to immediately make regulations or formulate code of conduct for the providers of electronic banking services, so as to ensure the privacy of customers and encourage the patronage of electronic banking.

5.2.2 EVIDENCE ACT

Section 93 of the Evidence Act should be amended to admit computer generated documents as primary evidence as recommended by the Law Reform Commission in their proposed “Evidence Act 1998", which is yet to be considered and enacted by the National Assembly.

5.2.3 CONTRACT LAWS

Electronic banking legislation must take cognizance of issues relating to encryption and digital signature to ensure that the legality and admissibility of such documents in the law court are not taken for granted. The evidence Act must necessarily be amended to allow for the admissibility of electronically executed document as primary evidence.
E-banking documents must guarantee the following:

Authentication, Integrity, Non-repudiation and Confidentiality.

Encryption takes care of confidentiality while digital signature ensures authentication, integrity and non-repudiation.

5.2.4 CRIMINAL LIABILITY

In paper-based transactions involving cheques, persons who alter or forge a document may be charged for forgery. However in electronic banking there are no papers or written signatures that can fit into the definition of documents or writing under sections 463 or 464, of the criminal code especially as computer information does not exist in writing, and the customer's PIN is not a written document.

It is obvious that a person who engages in an unauthorized transaction in electronic banking may not be successfully tried and convicted for forgery especially as the provisions of the criminal code were not designed to deal with electronic banking.

It is therefore suggested that the proposed legislation should identify offences that are peculiar to electronic banking and provide for punishment accordingly.

The regulatory authorities should be empowered by the legislation to enforce relevant provisions of the Act and issue appropriate guidelines on e banking. As a stopgap measure and for purposes of setting parameters for electronic banking, a robust guideline must be put in place immediately. It is gratifying to note that the CBN has been clothed with the legal cloak under section 28(1) (b) of the CBN Act 1991 as amended and sections 55(1) (b) and 59(1) (a) of the
Banks and Other Financial Institutions Act 1991 as amended.

5.2.5 CONSUMER PROTECTION**:**

The common feature of e-banking environment in Nigeria is the absence of statutory or regulatory provisions to protect the consumer of the products/services. By and large the bank's customer is made to sign or execute standard forms of contract or agreements prepared by the bank, or non-bank financial institutions.

The magnitude of risks as well as benefits to consumers using e-money products vary across products but those risks may be classified into some general categories as those facing existing payment mechanisms. These may include risk of financial loss, malfunction of cards/terminals or merchant acceptance and unauthorized disclosure of information without customers consent.

However, banks generally should have clear responsibility to provide their customers with a level of comfort regarding information disclosures, protection of customer data

and business availability that approaches the level they would have if transacting business through traditional banking channels.

The banks providing e-banking services and customers availing of the same are currently entering into agreements defining respective rights and liabilities in respect of e-banking transactions. A standard format/minimum consent requirement to be adopted by banks may designed which should capture all essential conditions to be fulfilled by the banks, customers and relative rights and liabilities arising there from. This will help in standardizing documentation as also develop standard practice among bankers offering e-banking facility.

Customer privacy policies and standards should take account of and comply with all privacy regulations and laws applicable not only in Nigeria but also any other jurisdiction to which the bank is providing e-banking products and services. In view of the level of development of e- banking in Nigeria and because it will be difficult for Nigerian banks to be conversant with the privacy regulations of all countries (Internet banking by its nature being no respecter of international boundaries), it will be advisable to draw from the Indian experience and require banks at this point in time to restrict the provision of their e- banking services to customers in Nigeria and Nigerians abroad who might want to use such service to remit money home/execute projects at home.

The Nigerian Consumer protection Agency may have to take steps to protect the Nigerian consumer enjoying e-banking services. This may include the enactment of specific laws, as is the case in the US (the EFTA and Regulation E) or the establishment of self-regulation approach, as is the case in the U.K. (the UK Code of Banking Practice Good Banking) and Australia (Supervisory Commission) or the enactment of consumer protection laws.

Consumer Protection Council Act makes no provision with regards to electronic transactions.

In protecting the consumer, certain information must be provided by both the bank and consumer in conducting electronic transactions.

The mandatory things that should be provided by the bank includes:

(a) Properly authenticated documents. - Documents must be executed by both parties.

(b) Integrity - Document is not tampered with between being sent and received.

(c) Non repudiation- Parties cannot deny document.

(d) Confidentiality- Document can only be assessed by sender or receiver.

Some of the additional information to be supplied to the customer includes:

(a) Condition and procedures for exercising right of withdrawal

(b) Geographical address of the banks place of business where consumer may address complaints.

(c) Conditions for canceling contract if contract duration is unspecified or exceeds one year.

(d) Consumer has a right to withdraw without penalty or need to provide reasons within a week or three (3) months if supplier did not comply with its obligations to provide aforementioned information.

All these details to be sent in written and durable form (could be e mailed) to the consumer and must be received before or at the conclusion of contract.

5.2.6 ELECTRONIC FUNDS TRANSFER (EFT)

EFT has been defined in the UNCITRAL legal Guide on Electronic Funds Transfer (EFT) as " a funds transfer in which one or more steps in the process that were previously done by paper based techniques are more being done by electronic techniques".

The legal implication of Electronic Funds Transfer (EFT), are essentially similar to the legal problems associated with e banking generally. But of peculiar relevance are issues of finality of transactions, liability for errors, and recovery for mistakes or fraud. The trend in other jurisdictions is the enactment of appropriate Electronic Fund Transfer legislation. In Nigeria however no legislation exists yet to regulate EFT. The Clearing House Rules clearly do not have the capacity to deal with EFT and cheque truncation.

The committee recommends that appropriate legislation be enacted to regulate the EFT and related transactions.

6. RECOMMENDATIONS

6.1 ELECTRONIC BANKING RISKS

1. Banks should 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.

2. Banks should ensure that their Boards review and approve the key aspects of the bank's security control process.

3. Banks should 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.

4. Banks should take appropriate measures to authenticate the identity and authorization of customers with whom it conducts business over the Internet.

5. Banks should use transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions.

6. Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.

7. Banks should ensure that proper authorization controls and access privileges are in place for e-banking systems, databases and applications.

8. Banks should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.

9. Banks should ensure that clear audit trails exist for all e banking transactions.

10. Banks should take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and/or stored in databases.

11. Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.

12. Banks should 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.

13. Banks should develop and make customers aware of the their privacy polices and privacy issues concerning the use of e-banking products and services.

14. Banks should 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.

15. Bank should ensure that Customer data are not used for purposes beyond which they are specifically allowed or beyond which customers have authorized.

16. Banks should 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.

17. Banks should take appropriate measures to ensure adherence to customer privacy requirements applicable to the Nigeria environment.

18. Only banks duly licensed and with physical presence in Nigeria should be allowed to offer e banking to Nigerian Residents. Therefore with this in mind virtual banks i.e. those that exist in the cyberspace should not be allowed for now.

19. The products/ services should not be offered to other jurisdictions.

20. 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.

21. All banks, intending to offer transactional services on the Internet/other e-banking products, should obtain an approval-in- principle from CBN prior to commencing these services. The application should be accompanied by:

a. A resolution of the Board of the bank approving the bank's intention to engage in e-banking service;
b. The reasons for choosing such business;
c. The potential penetration it seeks to achieve;
d. Detailed cost-benefit analysis;
e. A listing of products the bank seeks to offer;
f. The technology and business partners for the products, and all third party support services and service providers with their track record and agreements with them;
g. The systems and the skills and capabilities it has in this regard;
h. The systems, controls and procedures it has put or intends to put in place to identify and manage the risks arising out of the proposed e-banking activities and.
i. The features and detailed mode of operations.

22. The bank should also enclose a security policy with a certification from an appropriate qualified system security organization that the security measures taken by the bank are adequate and meet the requirements and that risk management systems are in place to identify and mitigate the risks arising out of the entire e- banking operations.

23. The CBN should hold discussions with the bank before granting such approval. After this initial approval is given, the bank would be required to inform the CBN of any material changes in website content in relation to launching of new products and advertisements.

24. Assurance about security controls and procedures should be periodically sought and obtained from the specialist external IT consultants/auditors, with the periodicity depending on the risk assessment of the supervisor.

25. Banks should be required to report every breach or failure of the security systems and procedures to CBN, who may decide to subject the failure to an on-site examination or even commission an auditor/ consultants to do so.

26. The CBN and NDIC as the supervisors should cover the entire risks associated with electronic banking as part of their routine examination. For this purpose, an e-banking examination checklist should be developed as well as e-banking examination procedures and manual.

27. Banks should review their security infrastructure and security policies regularly and optimize them in the light of their own experiences and changing technologies. They should educate their security personnel and end-users on a continuous basis.

28. Banks should develop outsourcing guidelines, which mitigate the risks of disruption and defective service in addition to complying with the "Guidelines on Vendor and Outsourcing".

29. The CBN should maintain close contact with the regulatory/ supervisory authorities of different countries as well as with the Electronic Banking Group of Basle Committee on Banking Supervision and review the proposed regulatory framework in keeping with developments elsewhere in the world.

30. The regulatory authorities should embark on an enhanced technical training for the supervisory staff to enable them cope with the challenges posed by electronic banking. This should as much as possible be complemented by appropriate attachment programs with other overseas regulatory/supervisory bodies.

6.2 INFORMATION TECHNOLOGY

1. CBN should monitor the technology acquisitions of banks, and all investments in technology, which exceed 10% of a bank's free funds, should henceforth be subject to the CBN approval.

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

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

4. Banks should be required to ensure that the implementation of the firewalls address the security concerns for which they are deployed.

5. 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.

6. Bank should be required to ensure that external devices permanently fixed on the network such as ATMs, PC's at remote branches, kiosks, etc. connected to the bank's network passing through the firewall must at the minimum be authenticated via Media Access Control (MAC) address in addition to other methods such as IP Addresses.

7. Banks should be required to implement proper physical access controls over all network infrastructures both internal and external.

8. Banks should be required to ensure that unnecessary Services (such as telnet, FTP, etc.) and Ports are disabled.

9. Effective physical security and appropriate environmental devices must be implemented at the location bank's Information System (IS) infrastructure.

10. Banks may be required to develop policies setting out minimum standards of physical security.

11. Banking applications run by the bank should be required to have proper record keeping facilities for legal purposes. It may be necessary to encourage banks to keep all received and sent messages both in encrypted and decrypted form.

12. When stored in encrypted form, it should be possible to decrypt the information for legal purpose by obtaining keys with owners' consent. Such information must be stored in conformity with existing legal requirements.

13. Banks should be required to identify an Information and Communication Technology (ICT) compliance officer whose responsibilities should include compliance with standards contained in these guidelines as well as the bank's policies on ICT.

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

15. Audit trail of individual transactions over the network must be kept with the bank.

16. Banks should have in place a security policy duly approved by their Boards. The security policy should address the following issues:

    a. Basic approach to information security measures.

b. The information and information 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.

17. All users and critical devices on networks used for e banking should be uniquely identified to facilitate arrangements for authentication, access control, confidentiality demarcations and enforcement of security policies.

18. 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).

19. All identities should be aged and renewed on expiry.

20. A minimum of two-factor authentication process should be required for all user access to the services provided.

21. Banks may need to consider the use of Public Key Infrastructure (PKI) for authentication of users for e-banking services.

22. Banks should introduce logical access controls over ICT infrastructure deployed.

23. 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.

24. Banks should ensure adequate back up of data as may be required by their operations.

25. Banks should also have, well documented and tested business continuity plans that address all aspects of the bank's business.

26. Settlement of e-payments transactions delivered through mobile telephony should be done through the banking system.

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

28. In view of the demonstrated weaknesses in the magnetic stripe technology, banks should be encouraged to standardize to the chip (smart card) technology within a time frame of 5 years.

29. For banks that have not deployed ATMs, the expectation is for such banks to deploy (with the approval of the CBN) chip based ATMs. 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.

30. Banks should be required to note that the Regulatory Authorities will consider fraud liability as a result of card scheming, counterfeit cards to be responsibility of the bank.

31. Banks should be encouraged to join shared ATM networks.

32. Banks should be required to display clearly on the ATM, the Acceptance Mark of the cards usable on the machines.

33. All ATMs not located in bank premises must be located in a manner to assure the safety of the customer using the ATM.

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

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

36. Non-bank institutions may own ATMs, however such institutions must enter into an agreement with a licensed bank, which should carryout the processing of the transactions at the ATM. The funding (provision of cash) and operation of the ATM should be the exclusive responsibility of the bank.

37. If an ATM is owned by a nn-bank institutions, processing banks must ensure that the card reader, 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 hereafter classified as confidential to the owner of the ATM.

38. ATMs at bank branches should, as much as possible, be located in such a manner as to permit access to the ATM 24 hours a day, 7 days a week.

39. Banks must ensure that when the ATM is accessed at hours other than when the bank is opened that access is granted to the ATM by a security staff of the bank or by the use of a card thereby limiting access to non-ATM customers.

40. Cameras used to record the activity of a customer at the ATM must not be able to record the keystrokes of such customer.

41. A telephone must be available to the customer to report incident at the ATM including inability to draw cash or other failures that take place. Such telephone line must be manned at all times the ATM is operational.

42. Point of sale devices deplorers, that place them 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.

43. Private companies may deploy Point of Sale terminals, however such companies should be required to sign agreements with banks that are responsible to the merchant for transactions done on the terminals.

44. 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 that is classified as confidential. A customers PIN number cannot be printed for any reason whatsoever.

45. Deplorers of point of sale devices should be encouraged to accept cards from other schemes.

46. Banks may subject to the prior approval of the CBN, issue international cards (such as Visa/MasterCard etc.) to their customers. Such cards however should be only be used outside Nigeria and payment on the cards should only be done through an ordinary domiciliary account of the cardholder or any other account that may be permitted by the CBN.

47. 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 Central Bank for the currency on the date of settlement.

48. Settlement of International Cards obligations should be done through the banking system. Third party (none bank) providers must first enter into agreement with financial institutions that will act as the settlement organization.

49. As switches connect consumers to their bank accounts to authorize transactions, only banks or a consortium of banks or agents for banks or banking consortium or any other company can act as a switching company, subject to the approval of the CBN. This provision is to minimize fraud and mitigate risk to the banking system.

50. Third party providers of switches 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.

51. The switching companies must meet the standards defined in the 3rd party service provider agreement. Third parties or service providers must meet

the guidelines as described under “Guidelines for Vendors and Outsourcing”.

52. Only deposit taking institutions duly licensed by the Central Bank can issue cards. Where cards are used in a closed environment, such as telephone cards used by a telephone company for it’s own customers or a fuel station issuing cards to its customer this is permissible. However any such card issued in a closed environment may not be used outside the closed group.

53. Only authorized financial institutions can undertake electronic transfer of funds.

6.2.1 INTERNET BANKING

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

2. Only authorized staff should have the ability to update or change information on the Web site.

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

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

5. 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.

6. 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.

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

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

9. 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.

6.2.1 VENDORS AND OUTSOURCING

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

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

3. When contracting for Electronic banking services, a bank should carefully consider how it intends to use third parties to design, implement, and support all or part of its Electronic banking systems.

4. Banks should 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.

5. Banks when outsourcing, should maintain control over the services and products provided by third parties.

6. When negotiating contracts, management of banks should ensure that responsibilities and accountability are clearly defined for each party.

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

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

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

10. Every bank should establish its rights, to the extent possible, in the event a third party fails to perform under the contract or fails altogether.

11. Banks should 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.

12. Banks should ensure that contract specify insurance to be maintained by the service provider.

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

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

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

16. Activity logs should be maintained to monitor remote vendor access to the systems.

17. Vendor software distribution procedure should be accessed for adequacy and each release accompanied by sufficient documentation.

18. Banks should notify the Regulatory Authorities of applicable service relationships relating to e banking.

6.3 MONETARY AND BANKING POLICY

1. The issuance of electronic money is likely to have significant implications for monetary policy, particularly in the future. It must be ensured that the price stability objective of monetary policy and the unit of account function of money are not endangered.

2. A significant development of electronic money could also have implications for the monetary policy strategy and the control of the operational targets, and this calls for re-examination of existing instruments so as to make them more robust.

3. Other issues such as the efficient functioning of payment systems and confidence in payment instruments, the protection of customers, the stability of financial markets and protection against criminal abuse, have to be taken into account.

4. Clear rules on the condition, under which electronic money can be issued and transacted, need to be established. Pursuant to monetary policy effectiveness, level playing-field considerations and in order to address some of the concerns on electronic e-banking, issuers of electronic money must fulfill some basic requirements.

6.4 LEGAL AND REGULATORY ISSUES

1. An all encompassing legislation on Internet/electronic banking should be enacted to address issues inclusive of privacy, encryption, digital signature, Domain Registration Penal provisions, issuance of guidelines on e-banking, consumer protection.

2. The amendment of relevant provisions of the Evidence Act to admit computer generated documented as primary evidence.

3. An Act on Electronic Funds Transfer (EFT) should be enacted.

4. Bill of Exchange Act should be amended to accommodate cheque truncation.

Banks should be required to:

1. Develop and make their customers aware of the their privacy polices and privacy issues concerning the use of e-banking products and services.

2. 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.

3. Ensure that Customer data are not used for purposes beyond which they are specifically allowed or beyond which customers have authorized.

4. 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.

5. Take appropriate measures to ensure adherence to customer privacy requirements applicable to the Nigeria environment.

7. CONCLUSION

The Committee recognizes that there are many issues relating to e-banking, and that some of them have assumed critical urgency. The Bank, therefore, needs to put in

place guidelines that would ensure that, the operation of e-banking does not limit the effectiveness of CBN's monetary policy operations, the risks associated with the channel are controlled, confidence in the banking and payment system is enhanced and market participants are fully protected. The primary objective should be to preserve the integrity of the payment system and to ensure that the role of the CBN in promoting monetary stability and managing a sound financial system is not jeopardised.

Technical Committee on E-Banking
10th February 2003

APPENDICES

APPENDIX 1

LIST OF MEMBERS -TECHNICAL COMMITTEE ON ELECTRONIC BANKING

1. Mr. C. O. Odiaka	Dep. Director, BOD, CBN (Chairman)
2. Mr. W. W. Ahrey	Dep. Director, ITD, CBN- Member
3. Mr. S. M. Onekutu	Asst. Director, Legal Dept, CBN- Member
4. Mr. K. A. Bamidele	Asst. Director, ITD, CBN- Member
5. Dr. (Mrs.) Iyabo Masha	Asst. Director, Research Dept, CBN- Member
6. Mr. I.S. Tukur	Bank Examiner, BSD, CBN- Member
7. Mr. Ayo K. Adeniji	Bank Examiner, BED, CBN- Member
8. Mr. G. M. Ladan	Manager, FOD, CBN- Member
9. Mr. Tayo Babatolu	Snr. Manager, FED, NDIC - Member
10. Mr. I. E. Essien	Manager, Research Dept, NDIC - Member
11. Mr. A. B. Zarma	Dep. Manager, OSD, NDIC - Member
12. Mr. M. Z. Ali	Dep. Manager, CSD, NDIC - Member
13. Mr. Alex Nwuba	MD/CEO, Smartpay Nig. Ltd - Member
14. Mr. Sadiq Abubakar	Head, IT, Valucard Nig. Plc - Member
15. Mrs. Zua Onubogu	AGM Legal, Smartpay Nig. Ltd - Member
16. Mr. F. G. Wasa	Bank Examiner, BSD, CBN- Secretary

APPENDIX 2

QUESTIONNAIRE

Introduction

Electronic Banking Committee with members drawn from CBN, NDIC and the Operators in the banking sectors was set up in 2001 with a view to drawing up a regulatory framework for the conduct of Electronic Banking (e-banking) in Nigeria.

To enable the committee achieve its mandate we hereby solicit for your cooperation by completing the questionnaire below. We undertake, in line with our usual practice that information furnished will be treated with strict confidentiality and will be used only for the purpose stated above. Your sincere and accurate responses to the questions are necessary, if we are to achieve our objectives.

Name of the Bank: -

Address of the Bank: -

Web Site Address of the Bank: -

E-Mail Address: -

1. Is your bank involved in e-banking?

[] Yes
[] No

2. If yes, please kindly indicate which of the following areas your bank is involved in: -

[] Basic Telephone Banking
[] Automated Teller Machine (ATM)
[] Internet Banking
[] All of the above
[] Others (state

3. In case you are rendering Internet banking services, who are your Internet Service providers (ISP)?

4. Where is your Web site hosted?

[] Locally
[] Overseas

5. Name the Country or State where the bank's Server is Located

6. What other area is your bank intending to go into in future with respect to e- banking?

7. What is the level of your bank's participation in e-banking?

[] Information Only
[] Information transfer system
[] Transactional

8. Does your bank have any security policy on e banking?

[] Yes
[] No

9. If yes, enumerate the various sections of the policy: -

10. Is your bank making use of one or a combination of the following security controls: -

[] Authentication
[] Firewall
[] Cryptography
[] Digital signature & certification
[] Certification Authority & Digital Certificate
[] Secured Socket Layer (SSL)
[] Public Key infrastructure (PKI)
[] Physical Security
[] All of the above

11. How often has your system (e-banking) been accessed by Intruders or unauthorised customers?

[] Very often
[] Often
[] Occasionally
[] Not at all

12. In case of system (e-banking) break down, does your bank have a contingency plan in place?

[] Yes
[] No

13. If yes, what is the nature of the e banking contingency plan and how effective is the plan?

14. How does the bank keep track of its customers or intruders that access your e-banking facility?

15. Does the bank have training program for staff that operate the e banking?

[] Yes
[] No

16. If yes, state the form or nature of the training: -

17. If no, why?

18. Please comment freely on any issues / areas you want the committee to incorporate into the proposed framework on the conduct of e-banking in Nigeria.