

# African Research Review

---

An International Multidisciplinary Journal, Ethiopia

Vol. 6 (2), Serial No. 25, April, 2012

ISSN 1994-9057 (Print)

ISSN 2070--0083 (Online)

DOI: <http://dx.doi.org/10.4314/afrrrev.v6i2.26>

---

## **Towards Effective Implementation of Electronic Banking in Nigeria**

(Pp. 290-300)

**Imiefoh, Pedro** - Computer Science Department, University of Benin,  
P.M.B. 1154 Benin City, Nigeria

E-mail: [pimiefoh@yahoo.com](mailto:pimiefoh@yahoo.com)

Phone: +2348034438481

### **Abstract**

*Businesses all over the world are transforming themselves into Electronic Businesses (E-Businesses) to meet the challenges of the 21st Century. Hence the current effort of the Banks in Nigeria aims at becoming efficient businesses in response to customers' demands. That is, delivers services more effectively and in so doing, reinforces revenue increase. The goal is to ensure a customer performs banking transactions electronically without visiting brick-and-mortar institution. These efforts are however not without significant challenges which stem from lack of e-readiness for e-banking. There is a widespread recognition that this challenge must be met by strategic building of infrastructures. E-Banking introduced projects often end in failure, either partially or totally. Therefore, stakeholders must be sensitized to the large gaps that often exist between project design and*

*Nigeria public sector reality. This paper highlights some issues of e-banking as well as strategies that may help to strengthen customer-bank relations for a better public service delivery and to close the design-reality gaps and thus improve e-banking project success rate in Nigeria. Also, it examines the significance of e-banking for more responsive and cost effective service.*

### **Background of Nigeria electronic banking**

Banking in Nigeria has come a long way from the time of ledger cards and other manual filling systems. Most banks today have electronic systems to handle their daily voluminous tasks of information retrieval, storage and processing. Irrespective of whether they are automated or not, banks in Nigeria by their nature are continually involved in all forms of information management on a continuous basis.

Electronic banking (e-banking) is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting a brick-and-mortar institution. That is, automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. Thus, the following terms refer to one form or another of electronic banking: personal computer (PC) banking; internet banking; virtual banking; online banking; home banking; remote e-banking and phone banking. Personal Computer (PC) banking and Internet or Online banking are the most frequently used designations. It should be noted, however, that the terms used to describe the various types of electronic banking are often used interchangeably.

However, progressively over the years, banks in Nigeria have witnessed a lot of regulatory and institutional reforms. In the recent past, the Central bank of Nigeria initiated reforms largely targeted at reducing the number of banks in the country and making the emerging banks much stronger and reliable. This was as a result of heavy challenges faced by the banks. They include fraudulent practice and corruption, erosion in public confidence, poor capital base, persistent cases of distress and failure, poor asset quality, and so on.

In a bid to catch up with global developments and improve the quality of their service delivery, Nigerian banks have now invested much on Information and Communication Technology (ICT) and have widely adopted electronic and communication networks for delivering a wide range of value added products and services. That is, the banks have in the recent past transformed from manual to automated systems. Ledger cards systems have

been replaced with computer networks, thereby facilitating the practice of inter-banking and inter-branch-banking transactions.

The recent introduction of mobile telephone system in the country has improved access to personal computers and internet service facilities have also added to the growth of electronic banking. Integrating the customers into this process of intranet and extranet banking in Nigeria is far from been realized due to militating factors, such as, lack of e-readiness, internet fraud, lack of adequate regulatory framework for protection, and security.

### **E-Banking issues**

There is no contradicting the fact that the world today experiences a problematic e-banking service. Equally true is the fact that over the years, the underlying issues have not been adequately addressed for the attainment of the objectives of e-banking. This has seriously affected and is still affecting the process of e-banking worldwide, particularly in developing countries such as Nigeria. This has elicited the reactions of many scholars with varying and often conflicting views on the fundamental issues at stake; how they can be resolved; and the importance of such resolution in the ever changing banking system:

#### ***(i) E-Readiness***

Cain (2004) forcefully argued that there is a great lack of strategic 'e-readiness' for e-banking in developing countries in particular. E-readiness has become sufficiently widespread as a concept to generate a number of variants in the successful implementation of e-banking. These include infrastructures, such as, data system; legal; institution, human, technology, and leadership and strategic thinking. These areas of e-readiness represent the strategic challenge to e-banking in Nigeria. They operate at the macro-level of the whole nation, and they act as a precursor to e-banking and its successful implementation.

#### ***(ii) Security***

For electronic banking to be effective in Nigeria, an area that must be addressed is security. For Information and Communication Technology (ICT) based services, the convenience associated with e-banking increases the need for security. That is, the core security areas, such as confidentiality, integrity, and availability must be addressed. A key concern is that of privacy. You cannot expect to do business on the net without addressing the privacy concerns of your customers. No customer wants to click away to a negative

balance. Security in e-banking is typically provided through the use of a user ID and password. These and other security measures must be installed and must be effective to prevent not only the breach of privacy but other security concerns like the alteration of data, ICT fraud etc.

System availability assurance still has a lot of effect on e-banking services in Nigeria. When you are an e-bank, your banking services are totally dependent on ICT. Of what use are powerful and operational programs, which are lacking in recovery procedures in an environment where telecommunications services are still at best epileptic? Fault tolerance and robustness of the ICT setup in a bank must never be underestimated. Contingency plans should be put in place to handle this persistent problem of availability. That is, as an e-bank offering worldwide services, the fault – tolerance of its ICT infrastructure cannot be compromised. Availability planning must address power supply, telecommunications, internet service, quality of technical support, backup facilities, and robustness of ICT setup, such as, hardware tools, banking software tools and networking systems.

### ***(iii) Plastic card and ATM fraud***

Modern technology has partly done away with the risks of carrying cash and the need for cash. Nevertheless, this has resulted in new fraud risks being incurred. The majority of the cards that are used in fraudulent activities have been either lost or stolen. They may have been stolen from homes, cars, offices, mail centres and so on. Frequent customers carelessness is making it far too easy for criminals to steal cards. It is essential that customers protect their cards and Personal Identification Numbers (PIN) for what they are and that is valuable. Treat your card and PIN like cash. Another reason for card fraud is that many customers fail to comply with the card issuer's requirement that PIN details are kept in a safe place and are not to be carried with the credit card. If the PIN can be committed to memory then the better, because the original PIN advice can then be destroyed. The card and PIN in combination is the customer's electronic signature and they must be protected.

There has also been a growth in counterfeit cards. Counterfeit cards are frequently based on details sourced from a genuine card. The genuine card details may be encoded onto another or several cards. An alternative method, where the genuine card does not permanently change hands is the use of the "skimming" technique. Skimming is where criminals gain access to merchant locations or technology, and then copy the magnetic information contained

on a customer's card which is later transferred onto a counterfeit card or cards. Another source of credit card details is via the internet where hackers using software programs are able to obtain card information and through trial or error can identify card issuers who do not put in place validation protection on their magnetic strips.

***(iv) Cheque fraud***

Cheques have been the subject of fraudulent activity in the banking system. The age of desktop publishing, scanners, laser printers has assisted fraudsters who have used these technologies to carry out their criminal activities. It has been stated that more money today is stolen from banks with a laser printer than a gun. From the banks' viewpoints, there are two main types of cheque fraud: The first is the situation where the customer is the victim. A criminal either steals or falsifies the customers' cheques. The second situation is where the customer and the criminal are one and the same. In this situation, the criminal opens an account with the intention of crediting and then drawing against worthless cheques. Banks in most cases face the increasingly difficult task of separating good cheques from fraudulent cheques. On the one hand, their role is to protect the assets of the customer and the bank. On the other hand, they need to provide fast high quality service to customers. The challenge is to find the correct balance between good customer service and risk assessment.

***(i) Advance fee fraud***

The Advance Fee Scheme or "419" is one of the most popular of all internet frauds. It has its origin from Nigeria in the 1980s. Its development and spread follow the path of the development in information and communication technology. At inception, postal letters were used as key media for committing 419 frauds. Later in the early, 1990s, it became integrated into telecommunication facilities, such as the telephone and fax. From the late 1990s, following the introduction of computers and Internet, 419 crimes became prevalently perpetrated through the use of e-mail and other Internet means. The latest dimension taken by the perpetrators of this crime is the use of fake Internet bank sites, and using that to encourage victims to open accounts with them.

These crimes are often targeted against banks and others. Frequently the "target" is asked to provide funds to cover "legal fees" or other "establishment fees" in order that the cache of account funds can be liberated and exported from the country. This scam involves bogus businessmen

seeking assistance in transferring substantial sums out of specific countries. This is a clear example of local vulnerability to global fraudulent scams. That is, fraud can be “marketed” globally. There is even global suspicion that a Nigerian crime syndicate that coordinates global crimes such as money laundering, bank fraud, and 419 scams exists today. These issues basically defeat the key ingredients of e-banking, which include confidentiality, integrity and availability.

**(ii) Internal fraud**

Internal Fraud is a very sensitive subject for any organization as there is frequently an aversion to bad publicity. Employee fraud in banks as in any organization may follow various approaches. With lower level employees, it will generally involve smaller amounts, e.g. manipulation or theft of petty cash. At the higher employee level it may involve much larger amounts. Types of defalcation fraud include diversions of funds or account manipulation, bogus loans, tellers, cash shortage, theft of traveller’s cheques and other valuables, theft of utility payments, and kickbacks. Understandably, banks have a policy of zero tolerance with respect to employee fraud and will ensure that offenders are sacked, prosecuted and funds resituated.

**E-Banking strategies**

The transformation of financial institutions which involves internal and external relationships through Information and Communication Technology (ICT) to optimize service delivery to customers is the most important element in the development of Nigeria as a nation. This involves the recent transformation of banks by the Central Bank of Nigeria to become responsive to customers demands, and the integration of ICT investments and strategic policies by the banks. Therefore, for Nigerian banks to successfully implement electronic banking to meet the demands of the customers, it is expedient to set in motion necessary mechanisms to implement the plan of action and adopt e-strategies:

**i. Personal computer (PC) banking**

PC banking is a form of online banking that enables customers to execute bank transactions from a PC via a modem. In most PC banking ventures, the bank offers the customer a proprietary financial software program that allows the customer to perform financial transactions from his or her home computer. The customer then dials into the bank with his or her modem, downloads data, and runs the programs that are resident on the customers

computer. Currently, many banks in Nigeria offer PC banking systems that allow customers to obtain account balances and credit card statements, pay bills, and transfer funds between accounts.

**ii. Internet banking**

Internet banking, sometimes called online banking, also known as virtual, cyber, net, interactive, or web bank, is an outgrowth of PC banking. Internet banking uses the Internet as the delivery channel by which to conduct banking activity. For example, transferring funds, paying bills, viewing checking and savings account balances, paying mortgages, and purchasing financial instruments and certificates of deposit. An internet banking customer accesses his or her account from browser software that runs Internet banking programs resident on the bank's World Wide Web server, not on the User's PC.

**iii. Transactional websites**

Transactional websites provide customers with the ability to conduct transactions through the bank's website by initiating banking transactions or buying products and services. Banking transactions can range from something as basic as a retail account balance inquiry to a large business-to-business funds transfer. E-banking services in Nigeria, like those delivered through other delivery channels, are typically classified based on the type of customer they support. Some of these services include retail services, wholesale services, account management, bill payment, cash management and so on.

Since transactional websites typically enable the electronic exchange of confidential customer information and the transfer of funds, services provided through these websites expose a bank to higher risk than basic informational websites. Wholesale e-banking systems typically expose banks to the highest risk per transaction, since commercial transactions usually involve larger currency amounts.

**iv. Account aggregation**

Account aggregation is a service that gathers information from many websites, presents that information to the customer in a consolidated format and in some cases; many allow the customer to initiate activity on the aggregated accounts. The information gathered or aggregated can range from publicly available information to personal account information, such as credit card, brokerage, and banking data. Aggregation services can improve

customer convenience by avoiding multiple logins and providing access to tools that help customers analyze and manage their various account portfolios. Some aggregators use the customer-provided user IDs and passwords to sign in as the customer. Once the customer's account is accessed, the aggregator copies the personal account information from the website for representation on the aggregator's site, i.e. screen scraping.

Other aggregators use direct data-feed arrangements with website operators or other firms to obtain the customer's information. Generally, direct data feeds are thought to provide greater legal protection to the aggregator than does screen scraping. Banks in Nigeria are today involved in account aggregation both as aggregators and as aggregation targets.

**v. *Electronic authentication***

Verifying the identities of customers and authorizing e-banking activities are integral parts of e-banking financial services. Since traditional paper-based and in-person identity authentication methods reduce the speed and efficiency of electronic transactions, banks in Nigeria have adopted alternative authentication methods, including: passwords and Personal Identification Numbers (PINs); digital certificates using Public Key Infrastructure (PKI); microchip-based devices (smart cards); database comparisons (fraud-screening); and biometric identifiers.

These authentication methods vary in the level of security and reliability they provide and in the cost and complexity of their underlying infrastructures. As such, the choice of which technique to use should be commensurate with the risks in the products and service for which they control access.

**Significance of e-banking in Nigeria**

Today, Information and Communication Technology (ICT) plays a very important role in banking. The range of customer services provided by banks has increased as a result of improving ICT. The quality, range and price of electronic services are an important part of any bank's competitiveness in Nigerian banking system and in the global market place of today's business environment. The tangible and intangible benefits ICT provides to banks cannot be over emphasized.

However, for the effective implementation of e-banking system in Nigeria, the underlying issues as discussed earlier must be addressed. Analysts believe that banking fraud costs the nation considerably more than any other type of

crime. It has serious consequences for the nations, whether they be victims of fraud whose trust has been betrayed or consumers who are required to shoulder the burden of business losses through increased costs and services, (Russell, 2000). But it is challenging for banks in Nigeria to face skilled counterfeiters of identification documents, who may have substantial resources and who are intent on establishing an account using false identification. The banking system considers the increased sharing of information between parties on fraudsters at the time account applications are made, would have a significant impact on the level of fraud and effective implementation of e-banking in Nigeria.

The advent of the Internet has a significant impact on banking services that are traditionally offered by the branches to the customers. With the help of Internet, customers can do their banking activities anytime and anywhere as long as Internet access is available. Customers are not the only beneficiary of this new service in the banking system in Nigeria. That is, making use of the Internet banking, commercial banks may greatly increase their market coverage and better track customers as well. Electronic mail in banking system improves communication between individuals and the bank, within the bank, with the bank and external parties and between banks. Banking processes are made more efficient and cost effective by integrating other aspects of banking operations, such as treasury management and financial control.

### **Conclusion**

E-banking has already arrived in Nigeria, like in most developing countries today, and the number of e-bank initiatives is growing progressively. The issues and strategies analyzed in this paper have shown that e-banking has a key role to play in Nigeria's current and future development. That is, it can offer critical improvements to the efficiency and effectiveness of e-banking and probably offers critical future legitimacy for e-banking system. E-banking delays in Nigeria as the Western countries push ahead will only reinforce the historical patterns of inequality. The issue for Nigeria, therefore, is not 'if e-banking' but 'how e-banking'.

In addressing the 'how' this paper has shown that there must be both a strategic and a tactical response to the contending issues for e-banking in Nigeria if improvements and legitimacy are to be guaranteed. The strategic response needs to be one, at least, that addresses all of the key 'e-banking' questions posed earlier. Certainly, it is this generic approach that has been

adopted by key international agencies involved with developing countries' e-banking, such as UNICT Task Force and the World Bank. For an effective e-banking in Nigeria, therefore, the strategic response should be built on institutional, technological, data systems' awareness and commitment, human legislative and above all, leadership.

The design-reality gap challenge associated with e-banking initiatives, particularly the fraudsters, who, through their behaviour are complicit in the importation of inappropriate Western e-banking models and systems should be addressed by customizing the match between Nigerian reality and the designs. This approach will certainly reduce the failure rate and increase the success of e-banking initiatives in Nigeria. An effective implementation of e-banking in Nigeria is important in making banking system more responsive and cost-effective.

### References

- Cain, P. (2004). "Automating Personnel Records for Improved Management of Human Resources: The Experience of Three African Governments in Reinventing Government in the Information Age" R. Heeks ed, London: Routledge. Pp. 135-150.
- Carison, J. Furst, K. Land, W. and Nolle, D. (2001). "Internet Banking Market Development and Regulatory Issues". Society of Government Economist Conference 2000. Washington D.C. Available Online at <http://www.occ.treas.gov/netbank/SGEC2000.pdf>.
- Csonka, P. (2009). "Internet Crime", The Draft Council of Europe Convention on Cyber-Crime. *A Response to the Challenge of Crime in the Age of the Internet Security Report Vol. 16 No 5*.
- Daly, J. and Miller, R. (2006). "Corporation's use of the Internet in Developing Countries", International Finance Corporation, Discussion Paper, World Bank Washington, D.C.
- Gupta, A. and Stahi, D. (2007) "An Economic Approach to Network Computing with Priority Cleases" Under Review in Management Science, University of Texas at Austin.
- Microsoft (2003). "Electronic Business Issues for World Trade", Microsoft Corporation, White Paper, USA.

- Peter, Grand Grace, D. (2001). "Red Flags of Fraud: *Trends and Issues in Crime and Criminal Justice*", No 200, Australian Institute of Criminology, Canberra.
- Russel, G. (2000). "Crime and Criminal Justice: Measuring the Extent of Fraud in Australia," Australian Institute of Criminology.
- Sanusi, J. (2003). "Central Bank of Nigeria's Standpoint of Anti-Money Laundering Compliance" Speech at the Conference on Anti-Money Laundering in ECOWAS: Bringing the Anti-Money Require in Compliance with International Standards, Lagos, Nigeria.
- Smith, R. Holmes, M. and Kaufmann, P. (1999). "Nigerian Advance Fee Fraud: Trends and Issues in Crime and Criminal Justice," No 121, Australian Institute of Criminology, Canberra. Available on Online at <http://www.aic.gov.au>.
- Whinstone, A. (2005). "Planning for Competitive use of Information Technology in Multinational Corporations". AIB UR Region-Conference Paper.