ELECTRONIC BANKING AND FRAUD: ISSUES RELATED TO EFFECTIVE IMPLEMENTATION

Pedro Imiefoh

Abstract

Banking has come a long way from the time of ledger cards and other manual filing systems. Most banks today have electronic systems to handle their operations. The emerging trend in the banking services has elicited the advent of fraudulent activities in the banking systems. The question then is: 'how effective is electronic banking system with its associated fraud today?' This paper highlights some issues of electronic banking and fraud. It also examines the significance of these issues for effective implementation in the contemporary business world.

Introduction

The advent of the Electronic Banking (e-banking) has a significant impact on banking services that are conventionally offered by the banks to the customers. With the help of the e-banking, customers can do their banking anytime and anywhere as long as the Internet access is available. Hence the other name for this new type of service has been called "Electronic Banking" or "Internet Banking." It can be defined as performing financial transactions over the Internet through a bank's website. Customers are not the only beneficiary of this new financial transaction. Making use of e-banking, banks may greatly increase the market coverage and better track customers as well.

In spite of those advantages, e-banking has not been equally adopted in all parts of the world. In the United States, for example, 45% of all Internet users have been using some forms of e-banking services. But in China, only 15% of Internet users were reported to be using e-banking services. The figure is also reported to be lower in developing countries, such as Nigeria (Gupta and Stahi, 2007). This gives rise to some important questions: To what extent will e-banking be adopted around the world? What factors are driving or inhibiting its adoption? How can we speed up its adoption rate? Many researchers on e-banking have found the prevalence of frauds in this new service very useful in examining these questions. Computer fraud refers to any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

- altering computer input in an unauthorized way. This requires little technical expertise and is not an uncommon form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;
- altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions; this is difficult to detect;
- altering or deleting stored data;
- altering or misusing existing system tools or software packages, or altering or writing code for fraudulent purposes. This requires real programming skills and is not common; and
- other forms of fraud may be facilitated using computer system, including bank fraud, identity theft, extortion, and theft of classified information (Csonka, 2009).

It is against this background that this paper attempts to examine critically the contending issues in the e-banking services and frauds with a view to enhancing and sustaining the objective in the business world. To achieve this ultimate goal, the paper has a five– item structure and this includes: the introduction; a theoretical framework, which discusses e-banking and fraud in perspectives; an analysis of the fundamental issues for effective implementation; the significance of e-banking and fraud; and a conclusion that summarizes the central arguments of the paper.

Research Objective

The purpose of this paper is to determine those contending issues of e-banking and fraud and their relevance. This involves the following:

(i) identifying and analyzing those contending issues of e-banking and fraud; and
(ii) examining the importance of the issues for effective implementation.

Electronic Banking and Fraud in Perspectives

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 (Microsoft, 2003). Unfortunately, this has seriously affected and is still affecting the process of e-banking worldwide. 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 business world. From the foregoing therefore, attempts are made to review perspectives with the objective of understanding the substance of their argument and how relevant they are to e-banking services and business development process.

The first of these is held by those who have consistently and tenaciously maintained that e-banking, with its present defective implementation is an exercise in futility. The basic argument of this group of thought is that e-banking suffers from a technological imbalance which has been the bane of its full implementation and realization of the objectives. That this problem can only be resolved through adequate operational infrastructures for the dynamic technological innovations. Such operational infrastructures include telecommunication and power, upon which e-banking generally relies. Due to the inability of the banks to integrate their operations into the Internet development process, e-banking can be said to have less impact in the existing banking structure.

Other scholars taking this perspective are also of the view that many firms have had trouble recruiting and retaining employees with the technological, design, and business process skill needed to create an effective e-banking presence. The need then arises to address this fundamental issue so that the continued implementation of successful e-banking can be guaranteed on the basis of adequate operational technological infrastructures.

Another perspective is held by those who believe that the environment in which e-banking is conducted is full of unclear and conflicting laws and these militate against the full implementation of e-banking. According to this group of thought, laws that govern e-banking were written when signed documents were a reasonable expectation in any business transaction. Even the government regulators in many cases have not kept up with technological innovations and this has led to the current poor state of e-banking system. Businesses that operate on the net must comply with the same laws and regulations that govern the operations of all businesses. If they do not, they face the same set of penalties, such as fines, reparations payments, court-imposed dissolution, and even jail term for officers and owners (Microsoft, 2003). This explains why regulation has become of paramount importance in the entire e-banking development process to avoid bank frauds, forgeries, money laundry, insider abuse and erosion of public confidence.

Yet another perspective is that held by those who are of the view that instead of focusing on the technological and legal aspects of e-banking system, the economic aspects which examine the major issues from an economic perspective should be addressed. This group of thought argues further that as e-banking system progresses towards a full fledged market place, economic analysis will take on an increasingly greater importance. In the electronic market place, the same market players are engaged in the same economic activities. However, they assume online identities, set up virtual firms and webstores, communicate, search, advertise, and settle payment electronically (Whinston, 2005).

Which ever views one holds on this all important electronic banking and fraud, debate, the fact remains that contemporary business world in relation to electronic banking and fraud is in a state of critical ferment of which the balance of the contending issues can only bring about the much needed change in the business world.

Contending Issues of Electronic Banking and Fraud

Many innovations enabled by the Internet, such as Intranet Applications (IA), Open Electronic Data Interface (EDI), and On-line Marketing (OLM) have immense benefits to firms and

organisations. However, consumer oriented business involving digital as well as physical products lag far behind lofty predictions. While others deal with technologies, laws, and economics to cope with peculiarities of the internet, we would like to discuss more fundamental issues of the electronic banking and fraud as business infrastructures.

Security

For electronic banking to be effective, an area that must be addressed is security. For any Information Technology (IT) 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, IT fraud, etc.

System availability assurance still has a lot of effect on e-banking services. When you are an e-bank, your banking services are totally dependent on IT. 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 IT 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 IT infrastructure cannot be compromised. Availability planning must address power supply, telecommunications, internet service, quality of technical support, backup facilities, and robustness of IT setup such as hardware, banking software and networking.

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 have been stolen from homes, cars, offices, mail centres and so on. Frequent customer 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 valuables. 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 are 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.

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' viewpoint 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.

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 developments in information 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 boqus 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.

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 diversion of funds or account manipulation, bogus loans, tellers; cash shortages, theft of travelers 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 restituted.

The Significance of Electronic Banking and Fraud

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

However, for the effective implementation of e-banking system, the underlying fraudulent activities as discussed above must be addressed. Analysts believe that fraud costs the nation considerably more than any other type of crime. It has serious consequences for all 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 to face skilled counterfeiters of identification documents who may have substantial resources and who are intent on establishing an account using false identification. These criminals will attempt to circumvent any difficulties placed in their way. The banking industry considers that 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.

Conclusion

We have attempted to examine the issues of importance generated by electronic banking and fraud with a view to addressing the need for effective implementation. It is against this background that we situate the importance of e-banking and fraud within the context of these issues in contemporary business world.

The manifestations of this focus indicate that e-banking and fraud are as a result of the development and spread of Internet services across countries. One of the most critical areas where the

impact of the change is being felt is the structure and instrument of banking operations. Therefore, to reduce frauds in e-banking systems, is to get the relevant local laws in place and in consonance with international laws and conventions; banks should require the customer to produce identification at a bank branch prior to picking up a card; there should be an increased sharing of information on fraudsters and fraud typologies; ensure that all the major background problems such as poverty, corruption and bad governance are addressed; and provision of a climate of certain risk of prosecution' for those persons that carry out fraudulent activities.

References

Carlson, J. Furst, K. Lang, W.W. & Nolle, D.E. (2001): Internet Banking: Market development and regulatory issues, society of government economists conference 2000, Washington D.C Available Online at http://www. occ.treas.gov/netbank/SGEC 2000.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, S*ecurity report* Vol. 16 No. 5.

Daly, J. & Miller, R. (2006): Corporation's use of the internet in developing countries, *International Finance Corporation, Discussion Paper*, World Bank Washington, D.C.

Gupta, A. & 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.

Russell, G. (2000): Crime and criminal justice: Measuring the extent of fraud in Australia, Australian Institute of Criminology.

Sanusi, J.O. (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, June 3.

Smith, R.G; Holmes, M.N & Kanfmann, 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.

Whinston, A (2005). Planning for competitive use of information technology in multinational corporations. AIB UK Region- Conference Paper.