African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 6, Issue 4, 2023 (pp. 139-159)
www.abjournals.org

A THEORETICAL REVIEW OF THE INTERNAL CONTROL MEASURES IN PREVENTING E-BANKING FRAUDS IN THE NIGERIAN BANKING SECTOR

Edward Idemudia Agboare

Department of Business Administration, School of Management, Huazhong University of Science and Technology, Wuhan, China.

Email: edward.agboare@yahoo.com

Cite this article:

Edward Idemudia Agboare (2023), A Theoretical Review of the Internal Control Measures in Preventing E-Banking Frauds in the Nigerian Banking Sector. African Journal of Accounting and Financial Research 6(4), 139-159. DOI: 10.52589/AJAFR-3DS06EOH

Manuscript History

Received: 15 Aug 2023

Accepted: 5 Oct 2023

Published: 26 Oct 2023

ABSTRACT: *The developments in the field of information technology have changed banking business and the manner in which its customers transact significantly, bringing about more reliance on electronic banking transactions fondly referred to as "e-banking transactions". This has also changed the kind of risk both the banks and its customers are faced with, resulting in some significant losses reported; and calling for the need for sound internal control systems that can be applied on e-banking activities to reduce losses and inherent risk. This paper is a theoretical review of the expected characteristics of the internal control system required to combat e-banking fraud in the Nigerian Banking Sector. Related concepts, theories and studies around internal control and electronic banking and fraud were reviewed. To reduce the losses attributed to e-banking frauds, the internal control system over e-banking transactions and activities should not be postmortem like the traditional banking services, but among others, be online real-time, generating alerts as transactions occur, having a combination of proactive and reactive techniques and should automatically generate audit trails. The paper recommends that the Central Bank of Nigeria (CBN) as the apex regulator of the sector should biannually review the controls put in place by the banks to check e-banking transactions for adequacy, and apply appropriate sanctions where necessary. Technology is constantly evolving, hence, the need for consistent review of processes and procedures by the banks, who should continuously sensitize its customers on safeguarding access credentials, while creating avenues for immediate reporting and account restriction in the event of suspicious activities.*

KEYWORDS: Internal Control, Technology, E-banking, Fraud Prevention.

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 6, Issue 4, 2023 (pp. 139-159)

www.abjournals.org

INTRODUCTION

The financial sector is commonly perceived as a significant part of the economies of all nations, considering the role it plays in promoting growth and development, savings, cash flow regulation, foreign exchange, trade, investment, capital accumulation, and so on. Therefore, in planning its growth and development, nations pay close attention to the financial sector. In recent times, there have been discussions centered around financial technology and banking, because with the advancement in technology around the globe there is a vast change in the way banks and their customers do business, as well as the running of national economies, which place more reliance on the use of electronic media. This has given the banking sub-sector, and the financial sector in general, a unique place; considering the roles and responsibilities it plays in intermediating in the economy.

These responsibilities also come with some downsides, and one of such is surviving the menace of fraud and fraudulent activities. Consequently, fraud prevention has become a central concern to banks, customers, and public policy makers (Sullivan, 2010). With this, security is a fundamental and increasingly important issue in today's banking industry (Kanniainen, 2010). However, losses and risk inherent in banking can be reduced by the planning, devising and implementation of a sound system of internal control.

The term internal control system as defined by the Institute of Chartered Accountants in England and Wales (ICAEW) is not only internal check and internal audit, but all systems of control both financial and otherwise, established by the management of an organization in order to safeguard its assets and promote operational efficiency. E-banking fraud is an issue being experienced globally and is continuing to prove costly to both banks and customers. Frauds in e-banking services occur as a result of various compromises in security, ranging from weak authentication systems to insufficient internal controls. In the light of the aforementioned, this paper is basically focused on reviewing the role of internal control system in combating electronic banking fraud within a service organization, with respect to safeguarding its assets, customers funds and ensuring efficient and effective operations in the Nigerian banking industry

Statement of Problem

In the words of Berney (2008), banks as well as customers rely heavily on the web for their banking business which has led to an increase in the number of online transactions. Gates and Jacob (2009) and Malphrus (2009) assert that the internet provides fraudsters with more opportunities to attack customers who are not physically present on the web to authenticate transactions. In the case of Nigeria, Chiezey and Onu (2013) stated that banking business has become more complex with the development in the field of Information and Communication Technology (ICT) which has also changed the nature of bank fraud and fraudulent practices.

Fraud and fraudulent activities pose a significant problem to the banking industry in Nigeria. The sector recorded a tremendous increase in losses to frauds from 2000 to 2014 (Nwosu, 2015). The Central Bank of Nigeria in 2014 in a bid to mitigate against the huge losses characterized by traditional banking services, and to liberalize the financial system in the country to align with global practices of fast and seamless transactions, increased its efforts to reduce overdependence on cash and enhance cashless transactions, implemented a cashless policy in the country, and arguably, since then, electronic bank fraud also increased.

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 6, Issue 4, 2023 (pp. 139-159)

www.abjournals.org

The Nigerian Deposit Insurance Corporation (NDIC) 2018 report disclosed that Nigeria's banks lost over N15.5billion (about $41.6million) to fraud, which was a huge leap from what the industry recorded as fraud losses in the previous four years (2014 – 2017, amounting to N12.3 billion); and about 89% of all financial service fraud happened through electronic channels, while only 11% was non-electronic. S.193 of the Cyber Crime Act provides that "Financial institutions must as a duty to their customers put in place effective counter-fraud measures to safeguard their sensitive information…", therefore, this paper intends to review the internal control measures essential in preventing electronic banking frauds in the Nigerian banking sector.

Objectives of the Study

The purpose of this paper intend to achieve is to review the qualities of the internal control measures needed in Nigerian banking sector in detecting and preventing e-banking fraud; other objectives this paper aims at achieving include: to identity the various types of internal control measures available and can be deployed by the bank management to combat e-banking fraud, to review the justification for these control measures employed, to highlight areas of weakness and make recommendations for corrective measures and procedure in securing the e-banking channels in the banking sector.

Study Justification

Inefficiency and improper control systems in some banks had led to their being declared as weak financial institutions (among other things). Looking at the current challenges faced by some banks in the banking sectors across the globe as the nature of doing business has drastically changed to sophisticated electronic devices and less paper. It is therefore essential that there should be yardsticks or models in relation to what a proper electronic based internal control system should be, in an important sub-sector such as the banking industry.

This paper helps create awareness on the inherent risk associated with electronic banking fraud and the caliber of internal control measures needed to check the menace of fraud in e-banking transactions and activities. For the management of the banks in Nigeria, this paper brings about increased awareness on the need to begin to establish a more aggressive system of accounting and other related control measures that can be applied electronically over the operations of their organization as a positive step towards detecting and preventing e-banking fraud.

Stakeholders in the sector also benefit from the study as it provides insight to the subject matter and its importance to the private and public sector. Academically, this study adds to existing knowledge on the subject of internal control and electronic bank fraud. This study will be found useful to students, lecturers and other scholars, as it will also serve as stimuli for further research in similar areas.

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 6, Issue 4, 2023 (pp. 139-159)

www.abjournals.org

REVIEW OF RELATED LITERATURE

We received such relevant views from numerous sources with regards to the various concepts, theories and empirical studies in such areas as it relates to the role of internal control systems in combating electronic banking related frauds.

Conceptual Review

Khanna and Arora (2009) opined that the recent rise in bank frauds calls for tightening of security mechanisms. A strong system of internal control is the most effective way of fraud prevention. The banks should increase their efforts to raise the level of security awareness in their organizations to combat frauds.

Internal Control Concept

It would be tough for any organization to protect its assets, rely on its records or operate in an efficient manner if there is the absence of a sound internal control system. Whittington and Pany (2001) state that the Committee of Sponsoring Organizations (COSO) defined internal control as a process designed to provide reasonable assurance regarding the achievement of objectives in the following categories: reliability of financial reporting; effectiveness and efficiency of operations; and compliance with applicable laws and regulations.

The Institute of Chartered Accountants of England and Wales (ICAEW) defined internal control as not only internal checks and internal audit, but all systems of control both financially and otherwise, established by the management of an organization in order to safeguard its assets and promote operational efficiency. International Auditing Guidelines (IAG) defined internal control as the whole system of control, financial and otherwise established by the management in order to carry on the business of the enterprise in an orderly and efficient manner, ensure adherence to management policies, safeguard the asset and ensure as far as possible the completeness and accuracy of records.

Internal control system as viewed by the American Institute of Certified Public Accountants (AICPA) is the plan of organization and all the coordinated methods and measures adopted within a business to safeguard its assets, and check accuracy and reliability of its accounting data, promote operational efficiency and encourage adherence to prescribed managerial policies (Obaseki, 2006). According to Ingram (2009), internal control are techniques employed by managers to ensure that specific control objectives are continuously met. Damagum (2005) puts, it simpler, as any mechanism that the management of an organization put in place to ensure adequate protection of the organization's assets against illegal use, thief and other fraudulent abuses.

From the above definitions of the concept of internal control, it is clear that internal control systems are medium (not ends on their own but a means to an end) through which organizations ensure smoothness in all their internal dealings as well as with outsiders.

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 6, Issue 4, 2023 (pp. 139-159)

www.abjournals.org

Components of Internal Control System

Internal control varies significantly from one organization to the next, depending on such factors as their size, nature of operations, objectives and the extent of geographical coverage. However, certain features are essential in considering the components that make up an internal control system.

The Committee of Sponsoring Organizations (COSO) stands on the framework of a good internal control system, including five components: the control environment, risk assessment, the (accounting) information and communication system, control activities and monitoring.

From a general perspective, internal control system in organizations can be developed around the following basic components;

- Internal Audit

- Internal Checks (checks and balances); and

- Physical Control (Damagum, 2005).

Objectives of Internal Control System

An entity's internal control system can be thought of as the nerve-center of its operations. Internal control techniques employed by organizations to ensure that specific control objectives are continuously met (Ingram, 2009). According to Bhattacharyya (2010), the main objectives of internal control is to set up an organizational structure where there is check and balances among departments as part of business process management and they include: reliability, conforming to regulations, avoid wastage, and safety of material and information.

In the opinion of Ingram (2009), common objectives of internal control systems include the priority of transactions, reliability of information, compliance with regulations, security and efficiency. More relied on by professionals with respect to internal control is the work of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. Accordingly, COSO sees the main objective of the internal control process as being categorized as follows:

- Efficiency and effectiveness of operations (operational objectives)

- Reliability and completeness of financial and management information (information objectives): and

- Compliance with applicable laws and regulations (compliance objectives).

Electronic Banking

Electronic Banking or E-banking as it is fondly called is a non-face-to-face contact banking service or non-physical contact banking service. Electronic banking services are the banking class of services that can be offered by a bank to individuals and companies through electronic means via a fixed or mobile telephone, and Internet (Ratiu, 2011). Given that internet technology has evolved considerably over the years, newly developed e-banking services now differ considerably from older systems (Khan & Mahapatra, 2009).

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 6, Issue 4, 2023 (pp. 139-159)

www.abjournals.org

Some of the more common types of E-Banking services today are Online Banking, Automated Teller Machines (ATM), Electronic Funds Transfer, Electronic Cheque Conversion, Direct Payment and Web ATM services, Mobile banking applications. Mobile banking apps payments are part of the technological new payment methods in Nigeria that is gaining wide acceptance. But in the view of finance professionals, consumers are chiefly concerned about the security of mobile payments and therefore are hesitant to wholly embrace it; this could explain the uncertainty surrounding the security of these payment methods.

Finance professionals themselves have numerous questions regarding mobile payments and the measures being used to safeguard those payments. There are also concerns about whether information is being transferred securely and if there is a risk of sensitive information being exposed. As mobile payments become equipped with security features such as tokenization and biometric authentication which do not impact their usability, they will be more widely accepted as a payment solution (McDonnell, 2015).

Fraud as a Concept

Black's law dictionary (4th edition, 1968 pp788) has defined fraud as, "an intentional perversion of truth for the purpose of inducing another, reliance upon it to part with some valuable thing belonging to him or to surrender a legal right. A false representation of a matter of fact, whether by words or by conduct, by false or misleading allegation or by concealment of that which deceives and is intended to deceive another so that he shall act upon it to his legal injury". Anything calculated to deceive, whether by a single act or combination or by suppression of truth or suggestion of what is false whether it be by direct falsehood or innuendo, by speech or silence, word of mouth, look or gesture (Kanu & Okorafor, 2013).

According to Watterston (2014), fraud is any deliberate deceitful conduct or omission designed to gain an advantage to which a person or entity is not entitled. It is the intentional use of false representations or deception to avoid an obligation, gain unjust advantage or in the context of public administration, commonly referred to as 'rorting the system'.

Fraud is perhaps the most fatal of all the risks confronting banks. The enormity of bank fraud in Nigeria can be inferred from its value, volume and actual loss. A good number of bank frauds are suppressed partly because of the personalities involved or because of concern over the negative effect such disclosure may have on the image of the bank. Customers may lose confidence in the bank and this could cause a setback in its growth (Chiezey & Onu, 2013).

Forms of Fraud

Adebisi (2009) states there are three forms of fraud. They are the internal, external and a combination of internal and external frauds.

a. **Internal fraud**: This is a fraud made against an organization by an insider- say a staff. If the staff is not capable of starting and concluding the whole process, he may carefully select a "TEAM" within the organization

b. **External Fraud**: This is a fraud perpetrated by outsiders. This is the exact opposite of internal fraud.

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 6, Issue 4, 2023 (pp. 139-159)

www.abjournals.org

c. **Combination of Internal and External Fraud:** This is often referred to as „‟collusion‟‟‟. Fraud in a bank can be committed by a bank customer, bank staff or a combination of staff and customer or third parties. This is very common and the success rate is higher than the first two. Fraudulent transactions in organizations such as banks could equally be classified according to fraud type. This in turn is divided into three broad categories, namely by flow, victims or by Act.

According to a 2020 study, there are three (3) types of electronic fraud in Nigeria, which corroborate the findings of Adebisi (2009) of fraud generally in the banking sector, which are Internal e-banking fraud, external e-banking fraud and collaboration between fraudsters and bank employees. Electronic banking fraud in Nigeria has increased since 2014 when the Central Bank of Nigeria (CBN) increased its effort to enhance cashless transactions.

Possible Causes of E-Banking Fraud

Adebisi (2009) pstated that there are many causes of fraud, depending on the enabling environment. The common ones under the following classifications:

- Social
- Technological
- Legal
- Personal; and
- Management; as we shall see under the theoretical framework.

Our focus here is the technological, as it is the backbone of e-banking fraud. We briefly stated them below:

(i) Continuous advancement in technology constitutes a major factor in enhancing fraud. The easier things become the more it is for fraudsters too.

(ii) The cost of perpetrating fraud using available technology is very low.

(iii) Technology facilitates near perfection of documents‟‟ replication.

(iv) It has turned the world to a global village. It has removed physical boundaries, hence fraud can be perpetrated along far distances

(v) Proceeds from fraudulent activities can be obtained with ease, e.g. via electronic money transfers.

(vi) Most of the technological fraudsters are youths with highly developed minds and are often influenced by successful peers.

(vii) Technological frauds are not easy to detect or prevent. There are so many user points worldwide where such frauds can be perpetrated.

(viii) Technological development is a continuous process. While a particular fraudulent act is being detected and prevented, other methods are being develop

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 6, Issue 4, 2023 (pp. 139-159)

THEORETICAL REVIEW

The following theories relevant to this study are hereby reviewed.

The Fraud Triangle Theory

Figure 1: Fraud triangle

Source: Researchgate.net

The **Fraud Triangle Theory** was propounded by Donald Cressey in 1950. Donald Cressey, a criminologist, started the study of fraud by arguing that there must be a reason behind everything people do. The fundamental observation of Donald Cressey (1919-1987), in the **Fraud Triangle Theory** was that fraud is likely to occur given a combination of three factors. This theory is made of a triangle of different fraud aspects that include perceived opportunities, perceived pressures and rationalizations (Chiezey & Onu, 2013).

Ngalyuka (2013) maintains that the term perceived is vital in the context that the pressures, rationalizations, and opportunities may not necessarily be real. Chiezey and Onu (2013) put forth that **financial and non-financial pressures** present the first temptation to commit frauds. Ngalyuka (2013) stated that 95% of the committed frauds are due to financial pressures such as debts, vices such as drug abuse and work-related pressures such to show good sales performance amongst others.

The second factor is **perceived opportunity.** According to Wanyama, (2012), the perceived opportunity is the ability of the potential fraudster believing that they can get away with the fraud or the consequences of being caught are manageable. Chiezey and Onu (2013) stated that the opportunity to commit fraud in the bank is characterized by employee access to assets and information that presents them with dual advantage of committing and concealing fraud. Kanu and Okorafor (2013) buttressed that these opportunities are presented through weak control

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

measures, lack of control measures enforcement, lack of sufficient punishment measures to act as a deterrence and inadequate infrastructure.

The last factor contributing towards frauds is the concept of **perceived rationalization**. This involves rationalization or justification of the fraud aspect as acceptable (Njenga & Osiemo, 2013). While Ngalyuka (2013) opined that rationalization refers to the justification that the unethical behavior is something other than criminal activity.

The Fraud Diamond Theory

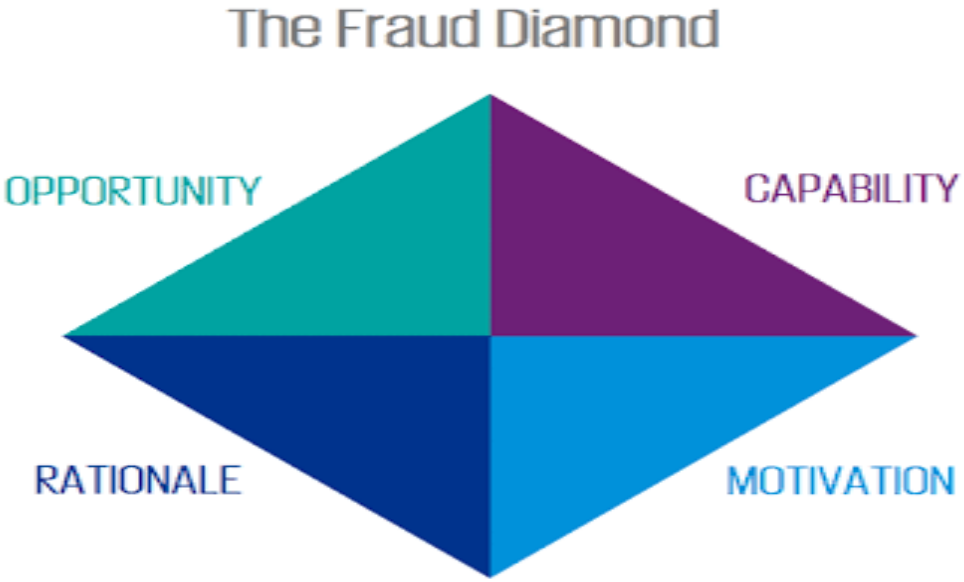

Figure 2: Fraud Diamond

Source: Karunia dhi.blogspot.com

The Fraud Diamond Theory was first presented by Wolfe and Hermanson in the CPA Journal (December 2004). It is generally viewed as an expanded version of the Fraud Triangle Theory. In this theory, an element termed capability has been added to the three initial fraud elements of the Fraud Triangle Theory. Wolfe and Hermanson (2004) argued that although perceived pressure or incentive might coexist with an opportunity to commit fraud and a rationalization for doing so, it is unlikely for fraud to take place unless the fourth element (i.e., capability) is also present. In other words, the potential perpetrator must have the skills and ability to commit fraud. This capacity often comes in the negative, where the fraudster lays hold on the access details of the owner of the funds.

In the Fraud Diamond Theory, an individual's capability, personality traits and abilities can play a major role in determining whether fraud may occur. While opportunities can open the doorways to fraud, incentive and rationalization will attract people to it, but such an individual must have the capability to recognize the open doorway as an opportunity and should be able to take an undue advantage of the identified loopholes.

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 6, Issue 4, 2023 (pp. 139-159)

www.abjournals.org

Other Relevant Theories on Fraud

We relied on the work of Kanu and Okorafor (2013) in considering other relevant theories on fraud.

According to the **Anomie Theory on Fraud**, in every competitive capitalist society, the other members of the society who are excluded from access to legitimate means to success and stardom will experience a sense of relative deprivation which they try to relieve by way of social vices like:

(1) Aggressive criminal behaviors, like bank frauds, and armed robbery attacks.

(2) Aggressive revolutionary behaviors like Coup de tat in the military and

(3) A retreat into psychosomatic illnesses like drug addiction, alcoholism, etc.

The Rotten Apple Theory opines that good and bad conducts within corporate organizations are infectious. Fraudulent actions by supervisors and top management can easily be emulated by their subordinates. Similarly, good conducts exemplified by top management will be emulated. This poses a challenge to management that whenever a "rotten and fraudulent apple" is identified in the organization, it must be quickly plucked off to ensure it does not contaminate the other good fruits on the tree.

EMPIRICAL REVIEW

Several researchers have attempted to classify fraud in various ways using different factors. Akwaja (2015) in his investigation of e-banking stated that Nigerian banks have lost a total of N199 billion to e-fraud between 2000 and 2014, mostly due to inappropriate and reckless management of customers' data. These figures have risen to N203 billion by the end of 2014 (Nwosu, 2015). Nwosu (2015) reported that the Central Bank of Nigeria's plan to establish an electronic fraud risk information center in collaboration with commercial banks in the country is a welcome development that should be fast-tracked.

E-banking also attracts varieties of fraud such as:

- Skimming (counter fact card fraud)

- Stolen card

- Fraudulent applications

- E-theft, never received issue

- Card data manipulation,

- Automated Teller Machine (ATM) video

- Spam mails or denial service

- Access swift fraud

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 6, Issue 4, 2023 (pp. 139-159)

www.abjournals.org

- Inter-bank clearing frauds

- Money laundering frauds; and

- Identity theft/phishing (utilizing other people's identity such as credit card info and identity numbers to make unauthorized purchases) (Chiezey & Onu, 2013).

In recent times, cyber-criminal activities across the globe have assumed such grave proportions that all enterprises - big and small, are exposed to security breaches and identity thefts of various kinds. Many of these crimes were found to have been caused by insiders in the organizations – such as disgruntled staff or greedy techies or sacked employees. Stolen identities seem to be the medium of hacking in many cyber-crime cases, inappropriate managing of passwords is alleged to be at the base of a significant number of cyber security threats.

Evolution of Electronic Crime

Electronic crime is alleged to have started in the 1960s in the form of hacking. The presence and availability of computers in the 1970s introduced new crimes as computer crimes in the form of privacy violation, phone tapping, trespassing and distribution of illicit materials. Subsequently, electronic systems crime emerged in the 1980s in the form of software piracy, copyright violations and introduction of viruses. The extent of damage after the 1980s increased due to the highly sophisticated electronic systems. These electronic crimes gave a wider impact on the international market, banking sector and other areas as well. Presently, electronic crime is a major subject of concern worldwide (Olufunke, 2010).

This paper looks at the data of online crime and many problems. Problems that banks and police forces face in controlling these crimes are enormous, considering the fact that data from the various regulators and agents of government reveal a continuous surge in the figures of losses as the years go by. There is a huge number of unresolved cases of e-banking fraud. In the opinion of this paper, significant improvements are possible in the way of dealing with online fraud, where the patterns of these frauds can be properly studied, to not specific identified loopholes for which solutions can be developed to mitigate any further occurrence.

Computers and the Internet are the most powerful tools in a row including financial networks, communication systems, power stations, modern automobiles and appliances. These computer networks records withdrawals, deposits, purchases, telephone calls, usage of electricity, medical treatments, driving patterns and much more. Quite a few innovative technologies are also extensively available which are responsible for causing electronic crime. They are denial of service attacks, viruses, unauthorized entry, information tampering, cyber stalking, spamming, paper-jacking, dumping or phone-napping and computer damage (Jain, 2005).

E-Banking Fraud

The Banking system is often referred to as the élan vital of any viable economy. Information Technology has become the backbone of the banking system. It provides a tremendous support to the ever-increasing challenges and banking requirements. Presently, banks cannot think of introducing financial product without the presence of Information Technology (Reddy, 2009). Electronic crimes are genus of crimes, through computers and its networks. Electronic crime is a crime that is committed online in several areas with e-commerce.

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 6, Issue 4, 2023 (pp. 139-159)

www.abjournals.org

A computer can be the target of an offence when unauthorized access of computer network occurs and on other hand it affects e-commerce. Electronic crimes can be of a variety of types such as:

- Telecommunications Piracy
- Electronic Money Laundering and Tax Evasion
- Sales and Investment Fraud
- Electronic Funds Transfer Fraud etc.

The Indian Banking sector is riding up with numerous revolutionary changes to transform the "Brick-and-mortar" bank branches to a modified network system in "core banking solutions". With this, a number of information technology-based banking products services and solutions are available – the most common IT based products available are Phone Banking, ATM facility, Credit, Debit and Smart cards, Internet banking, Mobile Banking, SWIFT Network, INFINET Network etc. (Bhasin, 2007).

According to security assessment of Nigerian banks, e-fraudsters had in recent years invaded Nigeria's banking platforms at will, deploying over 185 fake mobile applications on the websites of no fewer than 15 commercial banks in the country and in the process, extracted customers' personal and financial information with intent to defraud billions of naira from their accounts (Nwosu, 2015).

Credit card fraud has become ordinary on internet which not only affects card holders but also online merchants. Credit card fraud can be completed by taking over the account, skimming or if the card is stolen. The term "Internet fraud" refers usually to any type of fraud scheme that uses one or more components of the Internet, such as chat rooms, e-mail, message boards, or websites to existing fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to broadcast the proceeds of fraud to financial institutions or to other connected with the scheme (Ahuja, 2010).

However, of late, as stolen identities seem to have served as the 'hacking channel' for most of the cyber-criminals, analysts generally believe that improper management of the Administrative Passwords, which are often aptly referred as 'Keys to the Kingdom', is at the root of many security threats. Another harsh fact is that many a sabotage had been caused by the insiders of the enterprises. Either disgruntled staff or greedy techies or sacked employees were involved in many of the security incidents. That means, in this hi-tech era, breach of trust could occur anywhere, anytime leading to serious consequences.

Quite often, lack of well-defined internal controls and access restrictions pave the way for security incidents. According to Keltie (2009), most frauds are committed by or involve an insider, typically an employee in a position of trust. When an organization suspects that it is the victim of an employee fraud, often the first thing it does is launch an internal investigation - the initial action an organization takes when it suspects fraud can make the difference between recovering assets and protecting its reputation or breaking the law and being subject to prosecution, regulatory action or litigation.

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 6, Issue 4, 2023 (pp. 139-159)

www.abjournals.org

E-Banking Security Challenges

Online digital transactions challenge the concept of "isolated" basic business transaction cycles. The powerful software programs and fast transaction processing may bypass some of the traditional steps in manual transactions and empower individuals with additional necessary privileges. The potential loss of traditional controls, such as separation of duties, when coupled with the speed of transaction processing, challenges existing control and audit technology (Wang & Yen, 2005). The introduction of E-banking has come with its challenges. These range from technology adoption, financial limitations, and technology acceptance of new systems.

Other factors experienced globally are:

- The increase in security fears

- Cultural barriers

- Limited internet access, and

- Legislation (Masocha, 2010).

Auta (2010) found that security, user friendly, queue management, accessibility, time factor and fund transfer are major factors in the adoption of e-banking and that security is rated as the most important issue of online banking services.

Digital online transactions with their new set of characteristics demand new ways of control. Where the inbuilt controls or defenses are static, it creates an increasingly vulnerable situation as the technology changes. Even though they have once provided perfect protection from a system perspective, no security technology is perfect, particularly in a changing environment where systemic variety prevails, failure of the technology is merely a matter of time. Control and security systems that are not dynamic cannot fight against changing forms of threats and risks that are sometimes even worse than no control and security at all.

Often, the security systems capture the trust of the internet-based electronic banking user, but not function or continue to function as claimed as the environment changes. Mediocre security technology may eliminate the impetus for development and deployment of higher quality security technology. Therefore, the internet-based electronic banking internal control system should be designed in a more aggressive, preventive and proactive manner.

Data and payment breaches are increasingly more common, and vital business, financial and personal data are being compromised continuously. Malicious, ardent fraudsters are using more sophisticated techniques to circumvent various payment systems and target banks and their customers. Even when these criminals are unsuccessful in accessing direct funds, they often have been able to access confidential personal data, allowing them to steal identities of unsuspecting individuals and initiate other elaborate fraud attacks and breach even more secure payment methods (McDonnell, 2015).

Almost everyday, one can read of another example of cybercrime activity in Nigeria, whether in the form of an online banking fraud, embezzlement, intellectual property theft, or other criminal activity. Corporate investors certainly have a concern over this situation, as these cyber-crimes impact the bottom-line, but individuals and even the federal government should be concerned with the increasing number of cyber-attacks. Individuals like you and I have our

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

personal data at risk and can fall victim to various scams. Government understands that these financial cyber-attacks can undermine the economy (Mcmahonet al., 2015).

Need of E-banking based Internal Control

In 2010, most of the fraud cases were perpetuated via electronic banking systems therefore reflecting weaknesses in the internal control systems (CBN Annual Report, 2010). Financial services and organizations suffer yearly losses through crimes such as online banking, cheque and card fraud (Adams, 2010). These clearly indicate that criminals are exploiting e-banking mediums. Hence the need for improved continuous improvement in security to prevent fraud (Giles, 2010).

The online banking channel is the cheapest delivery channel for delivering banking products once established. Therefore, it is no surprise that the banks globally are continuing to shift towards e-banking services. With the growing patronage of e-banking services and its anticipated dominance in the near future, some of the known factors that contribute to addressing the acute problem of security must be addressed (Usman & Shah, 2013).

Internet-based electronic commerce is growing fast. The success and continued growth of internet-based electronic commerce is based on the technology development and business opportunities. For example, open and inexpensive access to millions of potential customers creates opportunities for companies planning to provide financial transactions and related services on the Internet. Enterprises that have implemented Internet-based applications as part of a business strategy have been successful in reducing business cycle time, improving cash flows, reducing inventories, decreasing administrative costs, and opening new marketing and distribution channels (Wang & Yen, 2005). The inadequacy of security potentially leads to financial losses, punitive measures by regulators and negative media publicity (Shah, 2012), therefore its importance cannot be over emphasized.

Internal control systems contribute significantly to the traditional businesses for assurance of safeguarding assets, providing assurance for the accurate and reliable accounting data, efficient operations, and for adhering to managerial and legislative policies. Computer security functions such as access control, logging and backup system also provide a mechanism to protect the business transaction system to certain extent. However, many traditional control and security mechanisms can be challenged on effectiveness and efficiency grounds in the new internet-based electronic commerce context (Wang & Yen, 2005).

Security is a fundamental and increasingly important issue in today's banking industry (Kanniainen, 2010). Consequently, fraud prevention has become a central concern to banks, customers, and public policy makers (Sullivan, 2010). Sidden and Simmons (2005) capped it when he stated that internal controls are the first and best defense against fraud. This therefore places emphasis on the role that internal audits are required to play to ensure compliance. Given the importance of strict internal controls, it is paramount that not only internal controls exist, but that they are strictly adhered to and policed by internal audits (Usman & Shah, 2013).

In its 2018 report, the Nigerian Deposit Insurance Corporation (NDIC) disclosed that Nigerian banks lost over N15.5B (about $41.6m) to fraud which was a huge leap from what the industry recorded as fraud losses in the previous four (4) years (2014 – 2017, N12.3b); and about 89%

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

of all the financial service fraud happened through electronic channels. S.193 of the Cyber Crime Act provides that "Financial institutions must as a duty to their customers put in place effective counter-fraud measures to safeguard their sensitive information…"

Characteristics of E-banking based Internal Control

The work of Wang and Yen (2005) was significantly relied upon in consideration of the characteristics an e-banking internal control should possess. The fundamental concepts of internal control can be applied no matter what data processing mechanism is used. When an organization decides to implement a new application or modify the existing one, control and security measures need to be analyzed. Many of these control measures will apply equally well to any operations platform: manual systems, computer processing systems, proprietary EDI or open Internet systems. These broadly applicable controls should be retained. However, because of the new risks of internet-based electronic commerce, some internal control processes need to be modified and expanded. Also, certain new controls and security measures need to be added where unique new risks are created in the Internet environment.

In this context, certain fundamental characteristics of the new electronic commerce environment should be considered when developing an Internet-based internal control system.

a. **Real-time:** Control activities and monitoring need to fit into a real time control and risk assessment environment. Since the transaction cycle is shortened in an Internet-based electronic commerce environment, the transaction data becomes more time-sensitive as well. Only real-time control can reflect real-time business conditions and protect the firm's resources.

b. **Integrated:** That internal control should be part of the design at the organizational level and transaction processing systems has been understood for a long time. However, in the Internet electronic commerce environment, this understanding must become a reality. For example, control mechanisms must be directly integrated with the reengineered business processes and transaction systems designed to achieve both control and efficiency in Internet electronic commerce. All control requirements including segregation of duties, authorization, approval and verification must be embedded in the integrated system.

c. **Automatic:** The higher the level and the more automatic the control, the more positive the influence the controls will have on the efficiency and effectiveness of electronic transactions processing and control. For example, the validity of data should be established before processing. This can be accomplished by using automatic front-end controls. Further, it is best to use computerized control procedures and sensors to automatically monitor on going transaction and asset disposition rather than traditional ex-post or sampling procedures. Automatic warning systems, reporting systems and even correcting systems should be built in as digitized control mechanisms.

d. **Dynamic:** Internet provides the dynamic information of business processes which presents an up-to-date business environment more accurately than less comprehensive traditional systems. Decision making in a dynamic business processes setting requires reliable and current information in order to reflect the real time situation. Being part of the monitoring mechanism, internal control, by itself, can be and should be dynamic as well. Internal control should take advantage of the availability of real-time control-related information. Control strategies and procedures should be dynamic not only to reflect up-

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

to-date business requirements but also to fit in real-time processing situation. Feedback controls should provide automatic inputs to digital notice and correction systems. Only flexible and dynamic internal controls can appropriately complement and support the dynamic Internet-based electronic commerce business processes.

e. **Reactive- and Proactive- Techniques Combined:** To complement real-time control requirements, mixed strategies can be used. The new technologies can be used as proactive enforcement controls, such as using automatic email to provide notice of a deadline or expected action. This contrasts with a transaction effectively requesting (reactive) appropriate controls, such as requesting and waiting for verifications. Combining these strategies increases the efficiency of control over efficient transactions.

f. **Preventive:** Due to the unpredictable and potentially severe consequences of system wide attacks, controls that rely on error detection and correction do not match the need of a real time system. To prevent errors rather than rescue after-the-fact requires that Reliability-by-Design modeling be applied in designing and implementing internal control mechanisms.

g. **Multi-Compensating:** It is important to maintain transaction integrity throughout transactions processing so that each transaction is completed and properly identified with its related entities. Any incomplete action in a transaction should trigger a compensating control response. Computerized control allows for the implementation of complex multiple-state compensation systems.

h. **Automatically Generated Audit Trail:** This entails online real time access, registration and transaction processing on the Internet, it is crucial to create transaction logs and audit trails automatically. This feature, properly used, will enhance the auditability of the Internet-based system. The above features of the Internet EC control environment can be exploited to strengthen firm-wide control. The new power of Internet-based internal control will support not only supervising real-time Internet-based business applications but also satisfying the requirements of sound security and assurance as to system performance and control.

Control Guidelines for User Identity and Password

There are several control guidelines that exist for users of e-banking channels but almost all have certain guidelines that have resemblance in terms of creation of user identity and password. The guides below are issued by **Friends bank** (these are similar to those the **Bank of Commerce** issued for E-banking fraud prevention best practices):

a. Create a “strong” password with at least 8 characters that include a combination of mixed case letters, numbers and special characters.

b. Change your password frequently. Friends Bank Online Banking will automatically require you to change your password every 90 days.

c. Never share username and password information with third party providers.

d. Avoid using an automatic login feature that saves user names and passwords.

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 6, Issue 4, 2023 (pp. 139-159)

www.abjournals.org

General Guidelines on Electronic banking

The below general guidelines were issued by Berkshire Bank for the e-banking consumers. These guidelines are similar to those maintained by most banks and financial institutions and can adopted.

a. Do not use public or other unsecured computers for logging into Consumer e-Banking.

b. Check the last login date/time, displayed in the upper left corner of the Financial Center page, every time you log in.

c. If the system does not recognize your computer or location, you will be asked to provide additional information to log into Consumer e-banking. This may include Out-of-Band Authentication via phone or SMS or answering more sophisticated (Out-of-Wallet) challenge questions.

d. Review account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and report any suspicious transactions immediately. Contact your local branch office or call your bank's Customer Service Center.

e. Whenever possible, use Bill Pay instead of checks to limit account number exposure and to obtain better electronic record keeping.

f. Take advantage of and regularly view system alerts; examples include: Balance alerts, Transfer alerts, Password change alerts, ATM/Debit Card alerts, Bill Payment alerts, etc.

g. Do not use account numbers, your social security number, or other account or personal information when creating account nicknames or other titles.

h. Never leave a computer unattended while using Consumer e-banking.

i. Never conduct banking transactions while multiple browsers are open on your computer.

Note: On Monday, September 18, 2023, Berkshire Bank launches a new, more modern online and mobile banking experience for their personal and small business banking customers.

DATA

The paper, a theoretical review of the internal control measures in preventing e-banking fraud in the Nigerian banking sector, relied on secondary data extracted from various sources ranging from articles, annual reports and various operational policies and procedural manuals and guidelines.

DISCUSSION

Internal control system, in the opinion of this paper, is a very vital part of any organization, be it small or large. Take away the internal control of an organization, and you have succeeded in opening it up to fraudulent practices, and might ultimately lead to the failure of sure an

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

organization. This was evident in the occurrences in the Nigerian banking sector about a decade ago, that lead to the collapse of some banks and the regrouping of other. With the advancement in technology, banks in recent times are seeking easier and cheaper ways to do business and therefore are embracing electronic banking channels the more.

This development has also come with its inherent risks, this also is evident in the volume of loses to e-banking in Nigeria from 2000 to 2014 (about N203 billion). Much has been written about internal control system, fraud and e-banking in Nigerian banking sector; however, to the best of my knowledge, little or no attention has been given to how internal control can be strengthened to help mitigate against the dangers associated with electronic banking. With such alarming figures going into record due to e-banking fraud, there is need for more knowledge creation in around the subject of automated internal control systems that are online-real-time and can help in combating the menace of electronic banking fraud.

CONCLUSION AND RECOMMENDATIONS

This paper highlights the role internal control system plays in the prevention of electronic banking fraud in the Nigerian baking sector. The essence of a sound internal control system is to ensure smoothness of an organizations activities, avoid errors (intentional and unintentional), prevent fraud and fraudulent practices, and discourage those with such intentions.

It is paramount to state that the competency and knowledge of the staff in the banks and the level of independence at which the components of the internal control systems are allowed to operate will to a large extent determine its effectiveness as well as efficiency. Therefore, like it is often said with external auditor, the primary function of internal control system is not the detection of prevention of fraud, but should it occur, it signifies a failure or weakness in the internal control system of an organization; and calls for more attention in developing measures that will bring about a sound internal control.

In view of the continuous development in information and communication technology (ICT) that is bringing more creative and innovative methods to the traditional banking operations, there is need for the systems of control to also be adequate to tackle any attempt to circumvent the process and defraud the banks or its customers; because fraudsters will continue to attempt to maneuver to breach the existing controls and access the banks system or scam unsuspecting customers.

While we often review past successes or failure to take decisions, they do not always guarantee the expected outcome, therefore, we put up the recommendations below, in addition to actions the banks and its regulator, the Central Bank of Nigeria, are taking to safeguard the owners of funds from having their fortunes flow into the wrong hands.

- It is not enough for the banks to establish electronic fraud risk information centers (referred to by most banks as “FRAUD DESK”), the Central Bank of Nigeria (CBN), being the main regulator, should annually or biannually audit the internal control measures put in place by banks over e-banking transactions for adequacy; and review the activities of those centers to ensure the right data is collected and managed, availability of the data as well as tracking down cases of e-banking frauds.

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

- The banks should create a separate unit of internal control equipped with staff that are knowledgeable in information technology to handle the internal control of its various electronic delivery channels.
- The banks should continually sensitize their customers on the need to ensure their information are kept secret and not shared with anyone, and where they have divulged such, they should immediately report same.
- The banks should provide available channels for customers to make urgent report on lost credentials as well as easy to use self-service medium for account restriction in the event of compromised credentials.
- Personnels are key to success, therefore, there is a need for training and retraining of internal control staff on latest developments in the field of information technology.
- Banks should enhance their communication mediums, such that online-real-time alert to customers once their account is being accessed, to ensure speedy blockage where access cannot be authenticated.
- Nigerian banks need to continuously review and upgrade their core banking solution/application to incorporate up-to-date features or accommodate automated control measures. Technology is constantly evolving, hence we will recommend consistent review of processes and procedures, as advancement in technology is giving the Nigerian banking sector a face-lift, to validate the necessity for a sound internal control system in combating e-banking fraud and to expand the availability of knowledge on the subject.

SUGGESTION FOR FURTHER STUDIES

The paper only focuses on the qualities of internal control measures needed to check e-banking fraud; hence, it is only an opener to a discussion that has a wide range of issues requiring the attention of the industry players, regulators and other stakeholders.

Conflicts Of Interest

The author declares no conflicts of interest regarding the publication of this paper.

REFERENCES

Adebisi. A.F (2009), *The bankers fortress*, Mega synergy Nigeria limited Lagos

Adams, R. (2010). Prevent, protect, pursue preventing fraud. Computer Fraud & Security, 2010, (7) 5-11 http://www.ebscohost.com

Ahuja, A.V (2010). Cyber Crime in Banking Sector. http://www.scribd.com

American Institute of Certified Public Accountants (AICPA), Committee on auditing procedure, internal control - elements of a coordinated system and Its importance to management and the independent public accountant, Statement on Auditing Standards No. 48 (AU320.27), AICPA, 1973

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

Akindele, R. I. (2011). Fraud as a negative catalyst in the Nigerian banking industry. *Journal of emerging trends in economics and management sciences.* Vol. 2(5), pp357-363.

Akwaja, C. (2015). Investigation: Nigerian banks lose N199bn to e-fraud. http://www.leadership.ng/news. Retrieved January 21, 2016

Auta. (2010). E-banking in developing economy: empirical evidence from nigeria. *Journal of applied quantitative methods*. Vol. 5(2)

Berney, L. (2008). For online merchants, fraud prevention can be a balancing act. *Cards & payments.* Vol. 21(2), pp22-27.

Bhasin, M. (2007). "Mitigating Cyber Threats to Banking Industry. *The Chartered Accountant.* April, pp.1618-1623

Bhattacharyya. M. (2010). Objectives of internal control. http://www.buzzle.com/articles.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric Authentication-A review. *International Journal of u- and e- Service, Science and Technology.* Vol. 2, (3)

Black, H.C. (1968). *Black's law dictionary* (4th Ed Rev). West Publishing Co.

Boynton, W.C. & Johnson, R.N (2006). *Modern auditing: assurance services, and the integrity of financial report.* USA: hermitage publishers.

CBN Annual Report, 2010

Chiezey, U. & Anu, A.J.C. (2013). Impact of fraud and fraudulent practices on the performance of banks in Nigeria. *British journal publishing*. Vol. 15, pp12-28.

Damagum, Y.M. (2005). *Auditing theory and practice* (2nd ed). Zaria: ABU press.

Gates, T. & Jacob, K. (2009). Payments fraud: perception versus reality – a conference Summary. *Economic prospectives*. Vol. 33(1), pp7-15.

Giles, J. (2010). The problem with online banking. New Scientist, 205, (2745) 18-19: http://www.sciencedirect.com

Hoffmann, A.O. & Birnbrich, C. (2012). The impact of fraud prevention on bank-customer relationship. International journal of business marketing. Vol. 30, pp390-407.

http://www.bankofcommercecefl.com

http://www.berkshirebank.com

http://www.coso.org

http://www.icaew.co.uk

http://www.thisdaylive.com. CBN tightens noose against e-banking fraud. Retrieved January 20, 2016

Ingram, D. (2009). Objective of internal control. http://www.ehow.com. Retrieved January 20, 2016

Jain .A (2005*). Cyber Crime: Issues & Threats and management.* Delhi: Chawla offset Press, p.1

Kanniainen, L. (2010), "Alternatives for banks to offer secure mobile payments", *International Journal of Bank Marketing.* Vol. 28 No. 5, pp. 433-434.

Kanu, S.I. & Okorafor, E.O. (2013). The nature, extent and economic impact of fraud on bank deposits in Nigeria. *Interdisciplinary journal of contemporary research in business.* January, Vol. 4.9, pp253-265.

Keltie, A. (2009). Preventing and investigating fraud in the work place. *Business crime*. http://www.bakernet.com

Khan, M. S., and Mahapatra, S. S. (2009). Service quality evaluation in internet banking: an empirical study in India. Int. J. Indian Culture and Business Management,2(1), pp.30-46

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH

Khanna, A. & Arora, B. (2009). A study to investigate the reason for bank fraud and the implementation of preventive security controls in indian banking industry. *International journal of business science and applied management. Vol. 4, pp1-21.*

Malphrus, S. (2009). Perspectives on retail payments fraud. *Economic Perspectives*. Vol. 33(1), pp31-36.

Masocha, R., Chiliya, N. and Zindiye S, (2010). E-banking adoption by customers in the rural milieus of South Africa: A case of Alice, Eastern Cape, South Africa. http://www.academicjournals.org. Retrieved December 30, 2015

McDonnell, N.K. (2015). Payments fraud and control survey. *Association of financial professionals journal.* http://www.afponline.org Underwritten by J P Morgan.

McMahon, R., Serrato, D., Bressler, L. & Bressler, M. (2015). Fighting cybercrime calls for developing effective strategy. *Journal of technology research.* January, Vol. 6, pp1-15.

Mercer, G. (2006). Audit internal control. Atlanta: Mercer university press.

Moore.T, Clayton.R & Anderson.R (2009). The Economics of Online Crime. *Journal of economic perspectives.* Summer 2009, Vol. 23□3□, pp.3-20

Nwosu, P. (2015). CBN's move to check e-fraud. http://www.sunnewsonline.com/new/cbn. Retrieved January 20, 2016.

Obaseki, O.O. (2006). *Elements of domestic operation in Nigerian banks*. Lagos: Begmeth 10 ventures.

Olufunke.O.O, (2010). Computer Crimes and Counter Measures in the Nigerian Banking Sector. *Journal of Internet Banking and Commerce*1, p.2

Online banking brochure general friends bank online guidelines. http://www.friendsbank.com. Retrieved, January 23, 2016.

Ratiu, C., Craciun., M.D., & Bucerzan, D. (2011). *Statistical model of the people confidence in e- business services*. Analele Universitatii Maritime Constanta, 51, 13(14) 237-240

Reddy.G.N, (2009). IT- Based Banking Services Enhancing Efficiency. *Financial Analyst.* November,p.69

Saddique, I & Richman, S. (2011). Impact of electronic crime in Indian banking sector. *International journal of information technology*. September, Vol.1, pp159-164.

Shah, M.H., (2012). Critical Success Factors in e-Banking: A Study of Two UK Retail Banks

Tilton, P. (2006). Guide to prevent work place fraud. http://www.chubb.com

Sidden, K. & Simmons, D. (2005). Banking on security. American City & County, 120, (11) 30 http://search.ebscohost.com

Sullivan, R.J. (2010). The changing nature of U.S. card payment fraud: industry and public policy options. *Economic Review*, Vol. 95 No. 2, pp. 101-33.

Usman, A.K. & Shah, M.H. (2013). Critical success factors for preventing e-banking fraud. *Journal of internet banking and commerce.* August, Vol. 18.2, pp1-14.

Wang, W. & Yen, Y.M. (2005). *General guidelines of internal control over internet-based electronic commerce*. Taiwan: APDSI, Taipei.

Watterston, J. (2014). Fraud and corruption control framework, 2014-2016. Australian national audit office

Whittington, O.R. & Pany, K. (2001). *Principles of auditing and other assurance services* (13th ed.). New York: Mc Graw Hill.

Article DOI: 10.52589/AJAFR-3DS06EOH
DOI URL: https://doi.org/10.52589/AJAFR-3DS06EOH