Electronic Banking System and Fraud Prevention in Nigerian Money Deposit Banks

AdijatuKuburatu ALIU
PG/MGS0710057

Being a Thesis Submitted to the Department of Accounting, Faculty of Management Sciences, University Of Benin, Benin City, In Partial Fulfilment of the Requirements for the Award of Master of Science (M.Sc.) Degree in Accounting (Forensic Option).

Supervisor: Prof. A. O. Enofe

September, 2019

DECLARATION

I hereby declare that the contents of this thesis are original work and no part of it has been copied or quoted from source(s) without full and adequate citation of that source(s) given to the original author(s) of the work(s) cited or quoted. I also declare that this work has not been presented for any award of a degree or publication elsewhere. I also declare that to the best of my knowledge liabilities arising from this work are entirely mine and not those of the supervisor.

AdijatuKuburatu, ALIU Signature and Date ……

CERTIFICATION

The undersigned certify that they have read this thesis and hereby recommended for acceptance by the University of Benin, Electronic Banking System and Fraud Prevention in Nigerian Money Deposit Banks, in partial fulfilment of the requirements for the award of the Degree of Master of Science in Accounting (Forensic Option), University of Benin, Benin City, Edo State, Nigeria.

Prof. A. O. ENOFE. ……
Supervisor Signature & Date

Prof. A. S. OMOYE. ……..……
Head of Department Signature & Date

DEDICATION

This research work is dedicated to God Almighty, Whom at all time is my all in all. Also, to the memory of my late father, Prince MukailaAliu and my amiable eldest sister, Mrs. Adegbite-Aliu Cynthia whom fate prevented from hugging me on this academic height.

ACKNOWLEDGEMENTS

I hereby register my profound gratitude to God Almighty Who gave me good health, excellent spirit and enablement in the course of my postgraduate journey. May He be praised.

I am indeed grateful to Prof. A. O. Enofe for the precious time he shared as my lecturer while also double as my supervisor- how would I describe him?He is a teacher and a father, his wealth of knowledge and understanding is immeasurable. God bless you for the sacrifices, pains, stress and dedication towards this work.

I appreciate all the lecturers from the Department of Accounting, Faculty of Management Sciences, University of Benin City, Benin City. I thank them for impacting in me this knowledge. To you, Prof. O. Omokhudu;I cannot thank you enough for playing the role of a father within the walls of the University of Benin. My Head of Department Prof. A.S. Omoye, I also thank you very much for every moment you offered. Prof. C.A. Okafor, how could I have succeeded without your advice. For Prof (Mrs) P.A. Isenmilaand Prof. Prince Famous Izedonmi, words are not enough to honour you as you were a mirror for academic emulation. I am indeed grateful to the Dean of the faculty,Prof. J.O. Ilaboya,and his Assistant, Dr. O. Omorodion; your support at the point of quitting won it all for me.To others Prof. S. Oladipupo, Prof. E. Dabor, Dr. K.O. Ogiedu, Dr. P. Ibadin, Dr. C.J. Mgbame, Prof.E. Eragbe, and Dr.J.O.Odia, thank you all. Also, your role can never be forgotten: Mr. Oboh Timothy and Mr.ObazeeUyi.

To my beloved husband, IfijehAndraq I am fully indebted to you thus far. May your reserves never diminish. My gratitude is incomplete without my mum-Mrs Joyce Tokpolor and also Mr Paul and Mrs Joy Ovuowo, Mrs Success Adesanya, Mrs Shakira James, Mr AliuIdris, Comrade Godwin Ifijeh, Engineer Sylvester Ifijeh, Mrs Veronica Ifijeh, Ifijeh Felix and

Ifijeh Clifford, Mrs Blessing Ifijeh-Gbadebo, Mr Alexender and Miss LilianIredia, and Miss AtonbaraOmbu.

I must say you brought me joy; First Bank of Nigeria especially Mr. KazeemAdelakun (RIP), MrsOgie-Darlington Josephine, Mr Aigbe Newton and Mrs Tina SegunIkusika, the Benin Siluko Branch team, Mrs Celina Imasuen, Mr EmmauelAfe, Mr AdeolaGbanini, Mr GbinosaDankaro and First East Circular Road team and to Mr FunmiladeMajeed and the entire Bezaleel Group.

TABLE OF CONTENTS

Abstract

The study examined the electronic banking system and fraud prevention in Nigeria deposit money banks. It adopts quantitative research methods with the aid of descriptive statistics, a demographic analysis of respondents, test for heteroskedasticity, test for misspecification, regression analysis; using the t-test, Ramsey reset test (R-Square), Durbin Watson test and the Cronbach alpha test with the use of questionnaire as a primary source of data. The theoretical framework was informed by theRoutine Activity Theory (RAT) and Fraud Management Lifecycle Theory (FMLT), two theories that emphasized the place of behaviour on fraud and the mitigating approach to fraud.

Findings of the study showed that the factors contributing to the increase of fraud in Nigeria electronic banking system is both technological and non-technological factors and put some fraud preventive measures as customer whistle-blowing, surveillance mechanisms, and technological mechanism.

The paper made the following recommendation: that workshops and seminars should not only be for bank staff, but also for bank stakeholders particularly customers and that customers should be kept abreast on tricks of fraudsters and how not to fall victim; individual banks should carryout training and retraining for staff on local and international content on e-banking channels since online fraud is borderless and remotely; banks should put in place sophisticated surveillance mechanisms for prevention of fraud; that Nigeria MDBs should take advantage of advancement in technological mechanisms like biometrics verification and authentication

CHAPTER ONE
INTRODUCTION

1.1 Background to the Study

In order to meet the insatiable quest for improved services delivery and better quality of life, technological innovation has created a new direction for businesses and style of living but the abuse of the internet, race for time, market, man imperfection and technology; combined with greed, have brought various challenges which must be tackled. The latter have manifested in various electronic fraud that has been perpetuated in form of password compromise, data theft, collusion, unauthorized funds transfer, credential hijacking, Automated Teller Machine (ATM) ramming, money laundering, phishing, etcetera resulting in electronic fraud (Boleigha, 2014).

The incidence of electronic fraud would increase, as fraudsters will habitually develop nefarious methods of abuse in order to profit from the emerging technologies fraudulently (Kuponiyi,2014). Ata and Seyrek (2009) opines that fraud is one of the major reasons for the failure of numerous banks causing damage to the deposit money banks and the capital markets thereby affecting an entire financial system. Fraud is a major setback to the entire financial sectors of any economy especially the banking industry as no bank is immune from it and also to all facets of life (Olorunsegun, 2010).

Electronic banking system, generally referred to as e-banking is the latest delivery channel for the banking services (Keivani, Jouzbarkand, Khodadadi&Sourkouhi, 2012). The Organisation for Economic Cooperation and Development (1998) pointed the benefits of sustainable electronic transactions for the global economy but warned its member economies on the severe impact this changing scheme could bring, one being the emergence of online threats (electronic fraud) to the detriment of consumers and users; as face-to-face client relationships

are often non-existent and this is so, as establishing one‘s real identity for electronic transactions is complicated, thereby making fraud easier (OECD, 1998)

The term ‘e-banking’ has been discussed in several ways by many researchers from diverse backgrounds, mostly because electronic banking involves quite a lot of banking activities through which customers inquire financial information and transact services usinga digital tap, mobile phone or computer systems (Hoehle, Scornavacca& Huff, 2012). Perkins and Annan (2013) describe electronic banking as the rendering of services and dissemination of information by banks to customers through various delivery channels that can be accessed with a personal computer or other electronic devices.

According to Wisdom (2012), the banking sector is now responding to globalization, innovation, customer needs and competition due to the development of a knowledge-built economy with the emergence of the latest information and communication technology, financial institutions particularly the banking industries have experienced thought provoking changes during the last decade.Adding, Wisdom (2012) asserted thatinformation and communication technology (ICT) has made athought provoking changes in the banking industry as it enhances banks’ ability to produce sophisticated products, streamlined superior structures, diversify their markets and expand globally. Furthermore, Darlington (1999) states that over the past three decades, customers’ needs have changed significantly with openness in their daily banking services together with maximum security and safety.Therefore, electronic banking has become a great business; the transformation from traditional banking to electronic banking has been a leap change (Wang & Huang, 2011).

Globally, the electronic banking system addresses several emerging trends as it has become very convenient and easy for electronic banking users to manage their bank accounts at any time and from anywhere in the world (Brar, Sharma &Khurmi, 2012). The banking sector has been strengthened by this development in recent years since electronic banking saves vast

amounts of resources in areas such as investments in ATMs, staff training, opening of branches and other operational costs (Chaturvedi&Meena, 2016). The internet has improved users' experience of electronic banking operations dramatically (Abu-Shanab&Matalqa,2015). Banking transactions arenow being performed in any place, anytime in the world through any bank delivery channel such as ATMs, POS, smart taps, personal computers and many more (Hoehle, Scornavacca& Huff, 2012).

E-banking activities have upgraded their business strategies in conformity with the internet. Banks have provided their services via the internet and thereby electronic transactions have increased speedily in the banking industry worldwide (Mahdi, Rezaul&Rahman, 2010). The advancement of electronic transactions gives tremendous prospective benefits to consumers and financial institutions in general (Singh & Singh, 2015).

Hoehle, Scornavacca and Huff (2012) asserted that the emergence of modern technologies have resulted inasignificant transformation of banking strategies and techniques as bank branches have started to lose ground to digital-generated banking services as the use of distant banking services has been augmented. Globalization, transforming social trends, competition and particularly information and communication technology advancements has brought intense reform into the banking system (Loonam&O'Loughlin, 2008). Generally, information infrastructure is considered worldwide as an opportunity for conducting innovative electronic distribution channels for bank products and services.

In contrast, fraudulent electronic activities are increasing and becoming more sophisticated, severely threatening; menacing the trust and security of electronic banking services (Mahdi, Rezaul&Rahman, 2010). E-banking fraud has turned into a thoughtful and serious phenomenon to the financial industry and crime managers across the entire globe (Rajdeepa&Nandhitha, 2015). These current electronic fraud opportunities are often tremendously difficult to mitigate due to their technological complexity; hence, banks may

devote substantial resources to prevent them but however; banks encounter challenges in preventing fraud and these challenges can often be aggravated by the organisational setting, political policies, regulatory frameworks and newly invented technology approaches in place (Kranacher, Riley & Wells, 2011). Nevertheless, even the issuing of momentous regulatory frameworks with governmental policies supports from many economies, it cannot be proudly said that theoccurrence of electronic fraud can be eliminated (Hoffman, 2002). But to Shannak (2013), in the very beginning of electronic banking systems, the scale of thefraud was very minimal because the banking industry was one of the most strictly regulated sectors. Equally, banking development from traditional banking to electronic banking is not only challenging in terms of managing bank risk but also filled with international and national irregularities (Chaturvedi&Meena, 2016).

According to Fadayo (2018), the incidences of electronic fraud is huge and some of the factors contributing to this increase include ineffective banking operations, internal control issues, lack of customer awareness, bank staff training and education, inadequate infrastructure, presence of sophisticated technological tools in the hands of fraudsters, negligence of banks' customers concerning their e-banking devices, lack of compliance with the banking rules and regulations, and ineffective legal procedure and the enforcement of rules and regulations in relation to the prosecution of financial fraudsters has been passive in Nigeria. These also corroborated with diverse types of security threats for both the electronic banking users and the banks – such as distributed attacks, phishing, identity theft, brute force attacks, spamming, credit card frauds, ATM frauds, hacking and unauthorized access, theft of service frauds, online money laundering, denial of service attacks, creation and distribution of malware attacks and other related online frauds are challenging issues (Fadayo, 2018).

E-banking fraud has created an aggressive presence in the banking sector and therefore, security cognizance is required to bring behavioural transformation, minimize employees'

vulnerability and guard against the prospective risk of fraud; and then create strong prevention measures using electronic technologies, adoption of fraud awareness and other new sophisticated anti-fraud approaches(Fadayo, 2018).

1.2 Statement of the Research Problem

Globally the incapability of the banking sector to effectively perform its functions as an intermediary and itsinability to control financial challenges have been a crucial concern to money deposit banks (Gertler&Nobuhiro, 2010). Rampini and Viswanathan (2010) statethat the main attribute of the deposit money banks is to collect deposits, make withdrawals, extend credits andrepresent stakeholders interest while monitoring the financial sector but however; banks need to protect the confidence and trust of their various customers (Wei, Li, Cao, Ou, & Chen, 2012).

The failure of banks to satisfactorily perform their fiduciary roles resulted from the numerous risks which are not appropriately controlled (Papazoglou, 2003). One of these risks which have progressively become a cause of burden in the banking sector is fraud (Sruthi&Prasanna, 2016). Furthermore, fraud means an intentional act of deception that makes society suffer damage either by monetary or physical asset losses is now a global menace (Ramamoorti, Morrison,Koletar& Pope, 2013).

It is truly worrisome that while the banking sector is persistently trying to contend with the demands of monetary authorities to recapitalise up to the required minimum standards, fraud perpetrators are always at work, decimating and threatening banks financial base (Mahdi, Rezaul&Rahman, 2010). The worrisome issue in Nigeria is the extent of involvement in the act of e-banking fraud by bank management staff and collusion with outsiders, as well as the ease at which bank electronic channels are being abused(Usman& Shah, 2013). According to Akindele (2011), fraud incidence in the banking system has become a problem to the Nigerian financial sector and it is obvious that anti-fraud agents and other law enforcement bodies are not able to

effectively get hold of perpetrators. On this note, Akindele (2011)observed that on average, money deposits banks in Nigeria was at a risk of losing millions of naira every working day because of the occurrence of frauds which happen in diverse ways.Even with the efforts of the Independent Corrupt Practices Commission (ICPC), Economic and Financial Crimes Commission (EFCC), also with other related regulatory agencies put in place to combat corruption and economic crimes in Nigeria, it is regrettable that little or nothing has been achieved (Aibieyi, 2007).

Mahdi, Rezaul, and Rahman (2010) undertake a study on credit card fraud detection in the banking sector: a focus on e-business where they asserted that credit card fraud in the banking sector has caused vulnerabilities in the entire online banking and that possible remedial action to detect credit card fraud must be considered. Chaudhary, Yadav and Mallick (2012) researched on fraud detection techniques: credit card and opines that when the term fraud comes into a discussion, credit card fraud clicks to mind. Their focus was mainly on credit card fraud and detection and agreed that fraud is a million dollar business and it is rising every year.

Adeyemo (2012) studied frauds in Nigerian banks: nature, deep-seated causes, aftermaths and probable remedies where they leaned heavily on the Nigerian Deposit Insurance Corporation (NDIC) annual reports for data and recommends that the battle against fraud lies on detection.Owolabi (2010) takes a review onfraud and fraudulent practices in Nigeria banking industry and put legislations as a control mechanism for reducing these frauds. Akindele (2011) researched on fraud as a negative catalyst in the Nigerian banking industry where he opines that fraud has caused many banks to collapse with many investors and depositors funds trapped and recommends adequate internal control system in order to control fraud.

Idowu and Adedokun (2013) evaluate the effect of monitoring and control activities on fraud detection in selected Nigerian commercial banks. The relationship between monitoring and fraud detection was examined, while the relationship between control activities on fraud

detection was also investigated and findings agreed there is a relationship and recommends that reviewing transactions after completion could be aneffective measure in identifying fraudulent activities. Nwankwo (2013) studied the implications of fraud on commercial banks performance in Nigeria and asserted that fraud has become a global phenomenon and that there is an urgent need for effective monitoring of banks e-channels such as ATMs for fraud. Alao (2016) took a look on analysis of fraud in banks: evidence from Nigeria and observed that the amount involved in fraud cases in Nigerian banks is a good determinant of banks 'failure and recommended that the service of forensic auditors should be sought in Nigerian banks to reduce fraud occurrence. Adedipe (2016) undertake a study on Nigeria internet fraud: policies/laws, changes that can improve effectiveness were relevant and legal measures available to help combat cyber fraud in Nigeria were highlighted while opining that the introduction, growth, use of the internet has numerous benefits but has however increase illegal activities in online banking. Agwu (2012) made a qualitative study on the problems and prospect of online banking in developing economies - a case of Nigeria and asserted that the dawn of the new millennium brought with it a plethora of activities that have impacted strongly on the academic field especially consumers' adoption of new technologies and recommended for more quantitative research to explore the problems and prospects of online banking in developing economies.

There existsinsufficient research studies on e-banking system and fraud preventionas researchers such as; Mahdi, Rezaul, and Rahman, (2010); Chaudhary, Yadav and Mallick, (2012); only examined causes of credit card frauds without an in-depth look at other frauds from major electronic channels such as computer, mobile tabs, digital web and telephones and worst is the fact that such discourse excluded prevention measures for fraud (it is better to prevent fraud than to detect because what is prevented no longer requires time, cost and effect).

Also, most studies done earlier in Nigeria on digital fraud like Owolabi (2010); Akindele (2011); Adeyemo (2012); Idowu, and Adedokun (2013); Nwankwo (2013), Odi (2013); Alao

(2016) and Adedipe (2016), amongst others were undertaken with a focus on detection, a survey on banks staff (without considering the customers who are the major victims of e-banking fraud), and most recommendations were on detection and investigation while excluding prevention as what is prevented need no detection or investigation. Agwu (2012), recommends more quantitative research be explored in the faceof problems and prospects of online banking in developing economies. It is on this note combined with gap on extants literature that we needtoempirically examinee-banking system and fraud prevention in Nigeriamoney depositbanks. Hence the following research questions:

1. What effect does customer whistleblowing have on fraud prevention in Nigerianmoney deposit banks?
2. What is the relationship between surveillance mechanisms and fraud prevention in Nigerian money deposit banks?
3. What effect does technological mechanisms have on fraud prevention in Nigerianmoney depositbanks?

1.3 Objectives of the Study

The major objective of this study is to examinethee-banking system and fraud prevention in Nigeria money deposit banks, while the specific objectives are to:

1. investigate the effect of customer whistleblowing onfraud prevention inNigerian money depositbanks;
2. ascertain if there is a relationship between surveillance mechanisms and fraud prevention in Nigerianmoney deposit banks; and
3. examine the effect of technological mechanisms on fraud prevention in Nigerian money depositbanks.

1.4 Research Hypotheses

The following hypotheses are formulated in line with the research questions and objectives.

The hypotheses are stated in their null form as follows:

H_{01}: Customer whistleblowing has no significant relationship on fraud prevention in Nigerianmoney deposit banks.

H_{02}: Surveillance mechanisms has no significant relationship onfraud prevention inNigerian moneydeposit banks.

H_{03}: Technological mechanisms has no significant relationship on fraud prevention in Nigerian moneydeposit banks.

1.5 Scope of the Study

This study focused on the money deposit banks (commercial banks) in Nigeriafinancial sector, the research questions as stated helpsin examiningthe impact of fraud prevention on e-banking system and on the bank stakeholders. The study covers the activities of both internal and external stakeholders of money deposit banks in Nigeriasince the core function of these stakeholders is to ensure an effective use of the e-banking system. Data were collected from customers of these banks and cross-sectional research design technique was employed.The 22 money deposit banks (MDBs) headquarters in Lagos and Abuja were used (CBN, 2018).

The selected banks were appropriate owing to our application of the Taro Yamani(1967) Method result and also on the homogeneity of the e-banking transactions.

1.6Significance of the Study

The research can likewise be projected to expose some of the literature regarding the understanding of fraud in the financial context. Given the application routine activity theory and fraud management life cycle theory along with other information from the research concerning the Nigerian banking sector, this can be regarded as significant research from this viewpoint.

There are also substantial practical applications of this study. The Nigerian banking sector can use the information generated from this study to modify its practices of combating fraud, and in addition to identify areas that are performing well. Investors and customers are the

major users of this information in a practical mode. One of the challenging factors is overseas investment fraud (Broadman&Isik, 2007). However, to some degree, financial risk is essential in almost all financial institutions. Understanding the level of risk and the specific factors that will need to be overcome will be tremendously significant for investors to make suitable decisions.

Moreover, the findings of the current study will be of interest for legal, regulatory and law enforcement institutions and policymakers within the executive and legislative arms of the Nigerian government; executive directors of Nigerian financial institutions; and all professional accounting and banking bodies. Also, corporate financial institutions will be able to design better control systems to curb fraudulent practices within their operations. The study will identify exposure to e-banking fraud and appropriate prevention approaches which will enhance national economic development, as the banking sector constitutes the backbone of the country's economic activities.

Finally, even though several studies have been conducted on e-banking fraud in various parts of the world, particularly in the United Kingdom and theUnited States of America, no broad study as regards fraud prevention has been done in Nigeria, as the ones conducted remained apiecemeal in data. It is therefore expected that this study will contribute significantly to the literature of the existing body of knowledge on e-banking fraud and the developing economy and immensely assist fraud examiners and forensic experts, especially in Nigeria.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter is to present the literature review of this study. It focuses mainly one-banking system and fraud prevention in Nigerian money deposit banks. The concept of e-banking system;e-banking fraud; nature of e-banking fraud; the contributing factors for e-banking fraud, e-banking fraud and prevention; review of fraud preventionvariable; empirical review and review of theories.

2.2 The Concept of E-Banking System

Electronic banking system, more commonly known as e-banking, is the newest delivery channel for banking services. It is a type of system through which customers can request information and execute transactions via telephone, digital television, computer or mobile phone (Deriga&Isac, 2014)

Daniel (1999) defines electronic banking system as the distribution of information and services by banks to customers through different delivery channels such as automated teller machine, point of sale, mobile banking, personal computer and other technological devices. Allen, McAndrew and Strahan (2001)refer to e-banking system as the supply of information or services by a bank to its customers using a computer. A common definition for electronic banking system comes from the Basel Committee on Banking Supervision where they define it as the provision of retail and small value banking products and services via electronic platforms as well as electronic payments and other wholesale banking services delivered electronically (Basel Committee Banking Supervision, 1998).

E-banking system represents a new age whereby delivering of services is through

automated channels such as personal computer and technological devicesto customers and it provides customers withan opportunity to gain access to their accounts, execute transactions, and obtain information on financial products and services through a public or private network, including the Internet (Deriga&Isac, 2014). Further, Deriga and Isac (2014) opines that there are several terms used in the literature and all refer e-banking system to mean: personal computer (PC) banking, internet banking, virtual banking, online banking, web banking, home banking, phone banking, remote electronic banking, mobile banking etcetera, but they are often used interchangeably.

According to Mobarek (2007), e-banking system has been around for quite some time in the form of automatic teller machines and telephone transactions but in recent years, modern e-banking system such as internet and mobile banking has revolutionized the banking services; and this can be traced to the early 1970s when banks began to look at these types of services as an alternative to some of their traditional bank functions butsuch a choice was considered appropriate since it ensures reduced costs as branches were very expensive to set up and maintain and secondly, e-banking products and services like ATMs and electronic fund transfer were an important qualitative element of differentiation for banks that used them (Mobarek, 2007). Given that banks operate in a fiercely competitive industry, their ability to differentiate themselves on the basis of price is limited. Thus, to remain on the market it is imperative for banks to adjust their strategies in response to changing customers' needs and developments in technology. The term e-banking became popular in the early 1980's referring to using a computer to access banking service via a phone line. E-banking first appeared in New York in 1981, where it was offered by major banks in that city, such as Citibank, Chase Manhattan, Chemical and Manufactured Hanover.

Banks from the United Kingdom started to adopt the concept in 1983 where the Bank of Scotland was the first to introduce it (Shannak, 2013). Electronic banking system hasstarted to

develop only since 1995, when American bank, allowed bank accounts to be opened online. In mid-2004, over 17% of Americans were already using electronic banking services.The increasing range and complexity of electronic banking services has led to the expansion of customers while satisfying more sophisticated needs and ensuring customer loyalty imposed a continuous demand for new technologies (Drigă, 2012).

2.3. E-Banking Fraud

Numerous definitions of fraud have been advanced in the extant literature. Abdullahi, Mansor and Nuhu (2015) define fraud asany act of expression, omission or concealment calculated to deceive another to his or her disadvantage, precisely, a misrepresentation or concealment concerning some fact material to a transaction that is made with knowledge of its falsity. Moreover, or in reckless disregard of its truth or falsity and with the intent to deceive another, and that is reasonably relied on by the other who is injured thereby.

Adeniji (2004) definedfraud as an intentional act by one or more individuals among those who manage organisation, workers, or stakeholders that result in a misstatement of financial records. MeenatKshi and Sivaronjani (2016) put fraud as an intentional set of deception involving financial transactions for the principle of personal growth. The Association of Certified Fraud Examiners (ACFE) (2010) defined fraud as a deception or misrepresentation that an individual or entity makes knowing the misrepresentation could result in some unauthorised benefit to the individual or the entity or some other party. In other words, mistakes are not fraud. According to the Economic and Financial Crime Commission (EFCC) Act (2004) fraud is an act undertaking to deviate from laid down legislation that are manifested in several forms like illicit money, extortion, corruption, narcotic drug, trafficking, engaging under-age, oil bunkering and unauthorized mining, evading tax, counterfeiting notes, piracy, open market abuse, dumping of toxic wastes and prohibited items (EFCC, 2004).

Wells (2014) defined fraud as unlawful gain through deception. Taylor (2011) argued, in

line with Wells, that fraud is stealing, disguising and obtaining personal gain from another person or a group of persons through deception. Curt's (2013) noted that fraud contains the acquisition of property or monetary advantage by way of deception, either concealment or misrepresentation. Boniface (1991), agreeing with the above three authors, described fraud as any deliberate act of illegal deceit, scam or forgery by a group of persons or a person to modify facts to gain unjustified personal economic benefit.

According to Graycar and Smith (2002), frauds usually encompass the transaction, falsification or forgery of financial documents and unlawful endorsement. KPMG (2000) observed that fraud occurs when a person or a group of persons of authority and responsibility refuse standard and violate the rules for the benefit of self-interest at the expense of others. In 1888, the United States Supreme Court accepted that fraud happens when there is a misrepresentation of a material fact by the defendant and the complainant sensibly believes it to be true. Entities, either as individuals or organizations, commit fraud to get a monetary advantage (Silverstone &Sheetz, 2007). Hence, fraud is criminal offences using deception for personal gain to the disadvantage or loss of another person. It comprises activities such as deception, concealment theft, money laundering, bribery, forgery, corruption, embezzlement, conspiracy, misappropriation, collusion, and extortion of material facts (Chartered Institute of Management Accountants, 2008).

Furthermore, fraud can be described as a deception and a false channel for converting another person's (legal owner) financial and non-financial property/assets for personal interest illegally. It can also be explained as a misrepresentation of financial statement which is intentionally done by internal or external stakeholders of an organization for personal motives. Bank fraud, then, involves the deceitful use of one's position without or within the bank for self-enrichment by intentionally misappropriating the bank's financial means, properties, or other resources held by the bank and collecting funds from bank accounts of customers (Taylor,

2011).

According to Graham, Li, and Qiu (2008) electronic fraud is a fraudulent act associated with an automated system by which someone aims to gain fraudulent benefit. Finch (2010) described electronic fraud as a fraud system that adopts internet components such as emails and websites to solicit information from potential victims to perform fraudulent transactions and transmit the proceeds of fraud to banks or other investment.

To Finch (2010), the differences in the definitions of e-fraud are attachable to certain factors such as the varied contexts in which e-fraud has been found to occur and therefore, electronic banking fraud can be elucidated as theft, robbery,forgery and altering of another person's financial assets illegally for self-motivated ends with the help of the internet. Electronic banking fraud can also be illuminated as a deception and dishonest way of converting another person's monetary advantage for personal benefit at the expense of others with the use of electronic devices and the internet.

Again, literature is satiated with distinctive styles of frauds. This view has been debated amongst scholars. Hamilton, Justin and Odinioha (2012) in the study titled, "styles of fraud" asserted that fraud styles are usually not exhaustive as fraudsters are forever devising new methods. Therefore, as societies and businesses are expanding progressive techniques of committing frauds are wearing new look (Pedneault, Silverstone, Rudewicz&Sheetz, 2012). The growth of businesses and rapid increased of the fraud perpetration are as a result of the development and expansion of the communication and information technology (Silverstone &Sheetz 2007).

Furthermore, Udoayang and James (2004) opined that fraud could be seen in two ways, viz. bite and nibble frauds. When an individual take assets and disappears in order not to be detected is known as bite fraud and that this style of fraud usually involves stolen of large assets

or huge amount of money and to escape being tracked down, the fraudster breaks out into a protected colony. Bite fraud can occur in the form of electronic frauds particularly, stealing of hardware devices or back-up devices of a computer system. While, an individual or fraudster involves in taking assets in piecemeal or small unit in order not to be detected easily is called nibble fraud. This style of fraud is very difficult to be detected at an early stage; hence, this kind of fraud occurs every day and is common in electronic banking frauds, particularly, fraud through mobile apps, ATM, POS, credit card and web banking fraud (Udoayang& James, 2004)

2.4Nature of E-Banking Fraud

The Nigeria financial system has witnessed several phases and dimensions of fraud, and this increasing rate has become a threat to the expansion of several financial houses and the sector aggregately (Nwankwo, 2005). Fraud in the Nigerian financial sector, especially the money deposit banks has taken a toll on the pillar of financial houses, causing distresses (Odi, 2013).

. Shongotola (1994) opine that frauds in Nigeria money deposit banks vary in nature, character and methods and that fraudsters adopt different ways to commit fraud. From perpetrators, Shongotola (1994) categorised bank fraud into three groups, which are: Internal fraud, External fraud, and Mixed Fraud. Shongotola (1994) asserted that the internal perpetrators of fraud are carried out by members of staff who are insiders and these persons may include accountants, executive assistants, supervisors, clerk (cashier), stenographers, technicians, drivers, and etcetera. On the other hand, external fraud are committed by persons not connected with the bank like an armed robbery attack either during the banking hours or during special movement of cash in transit and some external fraud could result through carelessness and recklessness or negligence on the part of some customers while mixed fraud are usually frauds committed by collusion between the insider staff and outsiders customers. It is a general belief that no successful fraud is perpetrated without the aid of an insider. Further,

Shongotola (1994) noted that the nature which fraud undertake under the perpetrators classification are inexhaustible as new ways are devised with time.

Furthermore, Alao (2016) group fraud styles into two, internal fraud and external fraud. When fraud is perpetrated by the individual employee or group of employees of an organisation or a bank using computer, point-of-sales, automated teller machine and internet inform of phishing, vishing and counterfeited or forged smart card is recognized as internal fraud. While, fraud committed with the use of bank financial records, customer's financial information and electronic devices such as ATM, internet, mobile app, mobile phone, pocket-picking machine by the outsiders, such as service providers, bank customers, suppliers and unknown party is called external fraud (Adewumi, 1986). The manner frauds are perpetrated in Nigeria money deposit banks as cheque Kiting, letter of credit fraud, advanced fee fraud, illicit money transfer, credit default fraud, financial instruments counterfeiting, account opening abuse, clearing interception, switching of telex and cyber fraud (Owolabi, 2010).

Iwuagwu (2000) argued that fraud perpetration can involve thecombination of both internal and external which known as outsider-employee fraud. This kind of fraud is difficult to detect because the insider-fraudster is asupplier of financial information needed and bank security information carrier to the outsider- fraudster who is an operator of fraudulent acts.

Additionally, ACFE (2015) argued that fraud against a business organisation can be perpetrated either externally by vendors, customers and other related parties such as individual or managers, employees, officers, and owners of the organisation. The author categorised frauds into three basic categories which are: external frauds, internal frauds and frauds against individuals. External frauds are kind of frauds committed by outsiders or third-parties by compromising electronic bank account through personal information about the victims. This fraud could happen through pharming, phishing and vishing. While, internal frauds also known as occupational frauds, can be explained as a means of using one's profession or occupation for

self or personal gain through intentional misuse or misappropriation of the company's resources. This kind of fraud happens when the executives, managers and other employees perpetrate frauds against their employer.

According to Iwuagwu (2000), fraudsters are progressing in the use of technologies and innovative approaches for concealment and perpetration of internal fraud schemes. While, fraud against individuals is a type of fraud in which many perpetrators have designed systems to de-fraud individuals such as identity theft systems, phishing systems, advanced fee crimes are just a few of the methods the fraudsters have discovered to defraud unsuspecting victims.

In the same vein, Adeyemo, (2012) opined that, fraud has been categorised in diverse ways and using various methods such as management and employee frauds, customer and non-customer frauds; and stakeholder and non-stakeholder frauds. Management Frauds are electronic fraud perpetrated by the top management of the organisation. These frauds can be committed through electronic financial statement and the victims of these kinds of frauds are creditors and investors (ACFE, 2015). This electronic banking fraud can be perpetrated through the creating of more investment from potential and current shareholder of the organization, doctor the financial statement, window dress the account statement and can also occur by painting the bank in better light in the sight of the regulatory authorities using electronic systems. Keivani, Jouzbarkand, Khodadadiand Sourkouhi (2012) explained that management fraud as the falsification of financial statements for the benefit of the person perpetrating the fraud. This involves false transaction, bogus trades, backdating of executive security or stock trade options and wrong use of corporate asset for personal benefits and violation of tax rules and regulations for personal gain using the internet and electronic devices.

While, Association of Certified Fraud Examiners (2010) concurred that management frauds happen through timing differences, fictitious revenues, improper asset valuation, inadequate disclosure and concealed liabilities and expenses. Employees' Fraud is generally

known as non-management fraud. It is a kind of fraud committed by the non- management staffs or employees of the organisation through forgery of customers' signatures, stealing of customer's passwords, PIN codes and electronic cheques for illegal withdrawal of money from the customers' accounts, creating and operating of fictitious electronic bank account, fund diversion, lending fictitious borrowers and other related computer's fraud or internet frauds (Adeyemo, 2012).

Furthermore, customers and non-customers' frauds occurred through the act of performing the primary functions of money deposit banks, which connects capital deficit customers with the capital surplus customers in the money market (Association of Certified Fraud Examiner, 2010). In the process of this, bankers come in connecting or interacting with both non-customers and customers and this leads to the risk of frauds. These types of frauds may be through counterfeit securities, opening of the fictitious electronic bank account, forged electronic cheque, fraudulent electronic money transfer because of a request made sole and solemnly through email, telephone, fax, telex, and other electronic means, and skimming card data (Regha, 2015).

While, stakeholders' and non- stakeholders' frauds is the kind of fraud perpetrated through the collaboration of insiders and outsiders, employees and non-employees, staffs and non-staffs of the organisation. Before this type of fraud to succeed, there must be an insider or internal fraudster that will be providing financial information while, the outsider fraudsters or external fraudsters will be carrying out the instruction given (Adewunmi, 1986). However, majority of banking functions in Nigeria are now electronically based activities including transaction of business such as funds, registration of new customers, collection of customers' data and preparation of financial statements, particularly in this era of cashless system, then, all types of fraud mentioned above are now electronic banking related frauds and there is need to discover the best way for preventing these menace.

Chartered Institute of Management Accountants (CIMA, 2008) differentiated frauds into several types which are also applicable to Nigeria economy. Frauds include the following: Frauds from any individual versus client; customers; consumers and others inform of misrepresentation of the quality of stocks or goods. Employee frauds versus employers inform of payroll frauds; thefts of cash; falsifying expense claims; false accounting and thefts of assets.In addition, frauds by the organisation, consumers; investors and employees inform of falsification of financial statement; selling of fake goods as original ones; not paying tax. Frauds by the company or individual versus government in the form of grant frauds; tax evasion; and social security gain claim frauds. Frauds by professional criminals versus big companies in the form of mortgage frauds; advance fee frauds; money laundering; counterfeiting and corporate identity frauds. Electronic frauds by a group of individual or an organisation with the use of computers and information technology through the help of internet to perpetrate frauds inform of spamming; phishing; social engineering frauds; hacking; and copyright (CIMA, 2008).

2.5The Contributing Factors for E-Banking Fraud

With the global use of progressively advanced internet technology, electronic banking is developing as a great medium or network for banking businesses (Chanson & Cheung, 2001). However, electronic banking fraud perpetrations are becoming more sophisticated, unbearable, greatly intimidating the security and trust of electronic banking activities. Agwu, (2012) viewed electronic banking fraud as an epidemic disease in the banking industry, which has become a great challenge to both management and customers of the industry. E-banking fraud has become a global and provocative issue that produces debate amid quite a few authors like Saleh, (2011); Pandey, (2010) opines that electronic banking fraud is a worldwide problem and is persistent to be overpriced to both banking sectors and customers.

Corroborating the views, Usman and Shah, (2013) put it that frauds in electronic banking services happen as a product of several concessions in security extending from

inadequate internal controls to feeble substantiation systems. Electronic banking fraud is now a thoughtful matter of financial crime management in all financial institutions. The development and advancement of challenging of electronic banking frauds such as ghost website, phishing scams and malware have coursed a massive loss in the banking industries worldwide (Wei, et al. 2013). Therefore, there is aneed to examine the causes of electronic banking frauds. Uchenna and Agbo (2013) stated that a lot of factors contribute to the menace of fraud perpetration in Nigeria, which is grouped into technological challenges and non-technological challenges. Ojo (2008); Idowuand Adedokun (2013) classified the causes of fraud in the banking industries into: the endogenous (institutional) challenges and the exogenous (environmental) challenges. Hence, for the benefit of this study, the factors thatcontribute to the increase of e-banking fraud were grouped into technological factors and non-technological factors which are explained below.

2.6 E-Banking Fraud Prevention Mechanisms

It is universally accepted that banking industries cannot escape from the menace of fraud as there are always some people who are motivated to violate the rules or commit fraud, and an available opportunity can make people perpetrate fraud(Subramanian, 2014). Therefore, there should be standard, adequate and flexible prevention techniques that can stand the course of time to tackle diverse changing fraud risks.

Bhasin (2016) noted that the Sarbanes-Oxley dictates that enterprises must be strictly devoted to internal controls measures and that systematic Sarbanes-Oxley compliance strength alone cannot offer complete security against the occurrence of fraud but proactive establishments of extra controls, as well as thorough approval of segregation of duties and procedures.

Adding this, Bhasin (2016) in a study titled “Combating Bank Frauds by Integration of Technology” stated that employees must understand the impact of the menace of fraud in the business. The employees need to identify the impact of deceptive behaviour and where and how

to document it. Furthermore, treasury officers need to be properly trained and legally informed on how to use the enterprise's fraud prevention techniques and tools. Bhasin (2016), George and Jacob (2015) stated that one of the most significant insecurity problems organizations encounter is fraud committed by dependable insiders and customers and that human resources department and cash control unit must perform background verifications on prospective employees and customers.

More so, Wells (2005), in the study “New Approaches to Fraud Deterrence”, found that fraud risk management policies and procedures are appropriate and significant for fraud prevention, detection and investigation and that there is a need for reporting policies, resolutions and procedures to be communicated to organizations’ employees. The author further suggested regulatory compliance, so as to ensure that suitable procedures and policies relating to company obligations for applicable and ethical conduct are in place, and to familiarize staff with the company’s standards and criteria for ethical conduct.

Bhasin (2016) stated that a-zero-tolerance policy plays a significant role in minimizing the menace of fraudulent incidences. Similarly, banks management should instantaneously take evidence or proof of suspected fraud to the law enforcement agencies.

Bhasin (2015), in an investigation into the “Menace of Frauds in the Indian Banking Industry”, found that the innovative prevention technology employed by some banks, including Data Glyphs, Two-Dimensional Barcodes, Biometrics, Cheque Image Processing, Data Analytics and Data Mining, contributed to addressing the problems of fraud and that therefore, banks need to discover and implement an appropriate sophisticated technique against fraud incidences.

Avinash-ingole and Thool (2013) posited that banks have different incentives and technologies for preventing frauds in e-banking services and that it is mandatory for every banking industry to have adequate rates of incentive and technology to protect customers from the menace of card payment fraud, compromised accounts, and identity doubtful. George and

Jacob (2015) presented a risk scoring model as one of the best prevention tools. This model centred on the current statistical data on card holders, related with the historical data with the cognizance that outdated method of authenticating via passwords and usernames is not going to be functional and effective in the contemporary system, which needs the support of unconventional technology. Therefore, George and Jacob (2015) concluded that money deposit banks in rendering electronic banking services must take advantage of fraud prevention software, smart card authentication, one-time passwords and biometric authentication. The authors further testified that biometric technology provides a better authentication technique and improves security.

Money deposit banks in modern technological age have put in place several technologies to fight fraudulent activities, one of which is the one-time passwords (OTPs). This is an indispensable technique, involving the display of a time-determine code which an e-banking customer needs to insert into the payment or deposit devices of the banking system (Johnson, 2008). The USB Tokens, PINs entry, cards and smart cards are other security instruments used by banks to verify e-banking customers through their custody of any of these security devices (Longo & Stapleton, 2002).

Another mechanism for electronic prevention is the transaction monitoring technique, a tool formed for a variation of bank card fraud deterrence. This technique investigates the receiver and sender of a transaction, compared it with previous fraud incidents and marks resemblance thereby alert for a declined or transferred to a call centre for physical authentication. This development involves no extra hardware for the customers as all examinations are performed in the setting (Longo& Stapleton, 2002).

Another preventive e-fraud mechanism is the Two-layered passwords which constitute a universal technique of fraud prevention for verifying customers before letting them gain access to electronic banking systems. For verification to be successfully completed, customers are

usually required to have separate internet banking passwords and usernames. Nevertheless, the regular use of a password for different prevention services leads to an increase in the vulnerability of electronic banking customers. Therefore, further methods of security are mainly for identity authentication (Moskovitch, Feher, Messerman, Kirschnick, Mustafic, Camtepe&Elovici, 2009). However, Vandommele (2010) concluded that the conventional approach of authentication with password and username is inadequate and unsatisfactory.

Biometric Approaches is considered a progressive means of prevention of electronic fraud and this involved various distinctive characteristics of electronic banking users revolving around recognition, verification and discovery. Vandommele (2010) discusses the various features of biometric technique: distinctiveness, universality, intransience, intransigence, performance, circumvention, satisfactoriness and adequacy. Sarma and Singh (2010) also emphasized the resemblance characteristics of biometric technology that should be given great concern in its analysis and evaluation. According to Bhattacharyya, Ranjan, Alisherov and Choi (2009), biometric authentication enhances the components of identification, non-repudiation and authentication in security information. This technology has a fundamental role to play in e-banking fraud prevention. Biometric systems provide a way forward by considering individuals' distinctive features as a means of identification. Even though recent development and improvement of biometric technologies, which include fingerprints, keystroke dynamics and iris recognition, appear promising, Sarma and Singh (2010) pointed out that authentication techniques for e-banking fraud prevention must be economically viable and technologically reliable. Many researchers, though, have proved the suitability and accuracy of biometric authentication for prevention of electronic banking fraud. Also, some organizations have implemented behavioural biometrics to enhance their security.

Bank verification number (BVN) is a mechanism used to reduce the potential harm of fraud, every business organization, particularly the banking industry, must invest not only in

advanced technology but also in policies and people for preventing attacks as promptly as possible and this has led the Central Bank of Nigeria to introduce the Bank Verification Number (BVN) in 14 February 2014, through the Bankers' Committee and in cooperation with all Nigerian Deposit Money Banks (DMB) and the Nigeria Inter-Bank Settlement System (NIBSS), aimed at protecting bank customers from identity theft and other financial frauds emanating in the Nigerian banking industry (Orji, 2015).

Globally, biometric technology has been adopted to analyse human characteristics as an improved form of verification, authentication and certification for real-time security methods (Blass &Oved, 2003). In the face of cumulative occurrences of compromising, of orthodox security systems (PIN and password), the need for sophisticated security for access to personal and sensitive information in the banking industry has become inevitable.

Another good key mechanism in preventing e-fraud is the Keystroke Dynamics. It is a method of analysing the user's approach to entering or typing personal information, passwords or accounting data in an e-banking channel by observing the keyboard input data (Monrose&Rubin, 2000). The key stroke approach is an innovative technique which was employed by the United States armed forces to differentiate friends from adversaries through Morse code and communication during the Second World War (Bartholomew, 2008). Over the years, there have been a number of studies on the relevance and reliability of keystroke dynamics through changing input process and algorithm procedures. Patil and Renke (2016) conducted experiments on keystroke dynamic technique via passwords ranging between six and eight characters. Revett, DeMagalhaes and Santos(2005) investigated keystrokes using a passphrase of a regular number of 14digits entered by every e-banking user. The authors calculated a resemblance measurement to form a decision chart and used this to evaluate the rules based on irregular sets. The surveys aimed to discover illegitimate and legitimate logins derived from the key-typing style of the e-banking users. These researchers' findings show (data

tests showed 95% accuracy achieved) that the first and last characters, including the typing speed, are the major indicators for determining legitimate and illegitimate logins. In addition, research conducted on conciliation between the standard password and lengthy text input using passphrases techniques showed a 0.5% false acceptance rate and a 3.1% false rejection rate and concluded that the keystroke dynamic system is gainful software that improves electronic system access protection; consequently, this makes it also appropriate for reinforcement of the internal security of banks (Revett, Magalhaes & Santos, 2005).

However, Gunathilake, Padikaraarachchi, Koralagoda, Jayasundara, Paliyawadana, Manawadu and Rajapaksha (2013) state that compared with other present techniques, keystroke dynamics are a highly efficient and prolific approach to validating internet schemes. Correspondingly, some scholars have argued that among the various biometric systems, the keystroke dynamic network is the best and most appropriate method due to its cost- effective implementation and performance (Choras & Mroczkowski 2007). Revett (2009) opined that some banks have implemented keystroke dynamics as a main authentication tool while others have used keystroke dynamics software as a supplementary authentication method

The bio-password is another type of preventive tools for the banks; it is a type of security biometric software that operates through a neural algorithm for examination of data and the provision of Crossover Error Rate (COER) to the users. If it provides 3% COER, this means the software has the capacity to register users instantaneously, steadily and noiselessly. Additionally, Shanmugapriya and Padmavathy (2009) investigated the intrusion of the waiting time between pressing an input key and obtaining a result differentiating legitimate e-banking users in order to differentiate the legitimate e-banking users from illegitimate users through the use of a multi layer neural network approach. The neural network approach is a forecast model using historical events to envisage the result of a future event. The outcome proved that adopting neural network for differentiation resulted in a better outcome than any other statistical

techniques.

Finally, ASSOCHAM (2015) in the investigation carried out on "Current fraud trends in the financial sector" found that the adoption of the following methods would prevent the rate of electronic bank fraud: whistle-blowing and tip-offs, suspicions transaction reporting, internal audit, data analytics, corporate security (physical and IT), investigative media and rotation of personnel. The author further explained that, fraud prevention oversight must be in place such as, surveillance (CCTV) and monitoring systems (escalation and investigation, data management, program and controls testing), analysing identified red flags, regulatory and internal reporting, internal audit, independent review and investigations.

2.6 Empirical Review

There are numbers of studies on fraud prevention in electronic banking (Phua, Lee, Smith & Gayler, 2012; Dzomira, 2014). Authors such as (Roberds, 1998; Vandommele 2010; Bhattacharyya, Ranjan, Alisherov & Choi, 2009; Tan & Rasiah, 2011) which adopted efficient and effective security control to prevent counterfeit transactions perpetrated by fraudsters and to enhance integrity and honesty transactions.

Some number of research studies on credit card fraud prevention has been conducted (Mahdi, Rezaul & Rahman, 2010). Studies on the prevention of electronic bank fraud have been carried-out using Neural Networks, Rule-Based Association System, Neuro- Adaptive Approach, Hybridization and other statistical modelling (Kou, Lu, & Sirwongwattana, 2004; Leung, Yan & Fong, 2004; Srivastava, Kundu, Sural & Majumdar, 2008).

Chiezey and Onu (2013) appraised the effects of fraudulent activities on the growth and development of banks through data from 24 Nigerian commercial banks, between 2001 and 2011, using secondary source of data and the association between fraud incidents and other variables were appraised using multiple regression analysis and Pearson product moment correlation. Moreover, some scholars based their studies on computer intrusion and prevention.

For instance, these studies mainly examined the prevention of anomaly and misuse of computer systems within the money deposit banks by monitoring program behaviour, multiple classifier models and neutral networks models (Beghdad, 2008; Ghosh, Schwartzbard, & Schatz, 1999; Eskin & Stolfo, 2007).

In addition, Mhamane and Lobo (2012) investigated prevention and detection of online banking fraud with the adoption of Hidden Markov Model (HMM) algorithm and Fraud Management Lifecycle Theory while, Wada and Odulaja (2012), Reyns (2013) and Leukfeldt (2014) conducted qualitative studies on cybercrimes and internet banking fraud with the use of routine activity theory (RAT) and fraud management lifecycle theory (FMLT). The finding holds that the combination of the absence of a capable guardian with a suitable target and a motivated offender in a convergence space and time has an influence on the victimization of malware and phishing. Precisely, Jamieson, Stephens and Winchester, (2007) investigated for fraud management and control with the use of fraud management lifecycle and their findings exposed that the proper interrelationship of distinct groups and components of these stages would result to successful control and perfect management of fraud in the organizations. Hence, the theoretical framework of fraud management lifecycle theory was considered also useful and appropriate for this study.

Likewise, Jansen and Leukfeldt (2016) researched on “phishing and malware attacks on online banking customers in the Netherlands”, the qualitative analysis of the factors of victimization with data collected from 30 victims of malware and phishing in their bank accounts through semi-structured interview and using routing activity theory as a theoretical framework. The finding showed that victimizations of malware and phishing attacks were marginally influenced by suitable targets. In the same vein, Hutchings and Hayes (2009) investigated quantitative research on “routine activity theory and phishing victimisation”. The study investigated 104 victims of deceptive email through the interview. The findings revealed

that probable victims who perform routine activities through online banking and other computer activities are more vulnerable to be defrauded by motivated offenders.

In a nutshell, the theory of routine activities has been extensively used in the extant literatures, among other things, robbery (Tseloni, Wittebrood, Farrell & Pease, 2004); sexual crimes(Tewksbury & Mustaine, 2001), cybercrime and online frauds (Newman & Clarke, 2003; Eck & Clarke, 2003; Wilsem, 2013; Pratt, Haltfreter & Reising, 2010, Williams, 2015; Reyns & Henson 2013). Likewise, Yar, (2005) and Choo, (2011) discussed cybercrime with application of mixed method and routine activities theory, thereby given boost to the ground for its adoption for the theoretical framework for this study.

Furthermore, the routine activity approach has been used by several studies of cybercrime (Duffield & Grabosky, 2001; Hutchings & Hayes, 2009; Reyns, Henson & Fisher, 2011; Van Wilsem, 2011). Therefore, the theory applies to this phenomenon. On the other hand, Pratt, Holtfreter and Reisig (2010) view through the suggestion of routine activity theory that those involved in e-banking is more likely to be victims of fraud. Karmen, (2010) opined that the victim of e-banking fraud is naturally involved in a lawful transaction and legitimate online business at the time of attack and oppression. Because of this, merely engaging in transacting business or transferring money (e-payment or e-commerce) from e-banking websites provide a high-fraud motive, compared to individuals or entities that do not transact business or pay money via e- banking.

2.7.1 Technological Factors

The introduction of electronic banking has come with its risks and challenges, starting from electronic banking adoption to financial transaction with the new system (Usman& Shah, 2013). The research statedthat several factors impacted the adoption and implementation process of electronic banking such as system security, accessibility, trust and social influence, the cost and time factors embedded in fund transfer, its usefulness and ease of use (Abu-Shanab,

Pearson &Setterstrom, 2019). Security is a factor that is frequently emphasized as a critical success factor (CSF) for the success and effectiveness of electronic banking. The deficiency of security will possibly lead to negative media publicity, financial losses and disciplinary measures by regulators. Security was ranked by some researchers as the significant concern of electronic banking operations (Yan, Md-Nor, Abu-Shanab, &Sutanonpaiboon, 2009).

Moreover, grounded in an empirical analysis completed on real-world transaction datasets, Kovach and Ruggiero, (2011) discovered that a lot of electronic banking accounts were defrauded by only one fraudster, which involved a small amount of money transaction with a total amount of money larger than one account. The author concluded that many frauds occur as a result of theincreased number of password failures which give opportunities to fraudulent behaviours. Correspondingly, in the survey carried out in Australian banks on electronic banking frauds, the finding showed that almost electronic banking frauds have the following challenges and characteristics, ineffective real time detection, weak forensic evidence, dynamic fraud behaviour, imbalance large datasets and diverse behaviour patterns of customers (Wei, Cao, Ou, & Chen, 2012).

Jassal and Sehgal, (2013) in their study titled “electronic banking security flaws” aimed at finding diverse types of faults in the security of electronic banking that end to loss of money by customers and banks. The authors discussed the reasons of security breaches and the involvement of both banks and customers in giving a chance to crackers and fraudsters to have access into their networks through web-browser installed on their customer’s personal computer which give opportunities to unauthorized persons to have access to their personal identification information and financial information (Nor, Shannab& Pearson, 2008). Usman and Shah, (2013) viewed electronic banking fraud as a global issue which is persistent to prove costly to both thebanking sector and its stakeholders. Electronic banking frauds happen because of different concessions in security started from feeble authentication systems with inadequate internal

controls.

Electronic banking fraud could be from bank website, such as cross-site scripting through malicious and SQL statement entered by attackers into the web page of the bank (Schneier, 2011). Omar, Sultan, Zaman, Bibi, Wajid, and Khan (2011) argued that most stakeholders willing to use electronic banking services because of its convenience, cost-effectiveness, speed and easy accessibility, but the finding reveals that ATM problems, electronic frauds and insecurity. European Central Bank (2014) reported that card fraud payment is one of the major means of fraud such as counterfeit card, card not received, lost and stolen cards. The author further elucidated that the contemporary mobile devices with their operating system were not intentionally produced with the security of financial payment, the transmission of personal data and sensitive payment through the use of radio technology leaks mobile payment to risks, unlike traditional payments, mobile payments expose include extra actor in the signal transmission such as mobile network operators and also, the general public may not have adequate awareness of the associated information security risks attachedto use of mobile devices and internet desktops or laptop for payment at home.

Correspondingly, Adedipe (2016) in his study internet fraud, findings show that the external fraud is fundamentally direct outcome of hackers' activities which include unauthorized access to electronic bank account information which are accomplished through pharming attacks, phishing attacks, session hijack, skimming attack, eavesdropping hijack, brute force attacks. These are emanated through bank staff and customers' ignorance and unawareness of common social engineering techniques, negligence in displaying PIN code and accounting information, and carelessness disposal of computer devices and related software.

Deloitte (2015) in the study of "India Banking Fraud Survey" discovered that there is increase in the electronic fraud occurrence in the banking sector because of lack of the tools and technology to discover the potential red flags. Likewise, Regha (2015) concord that difficulties

in preventing electronic banking frauds could be influencedby the following factors which involve: ineffective monitoring of electronic banking channels such as ATM terminals, internet banking, telephone banking, personal computer banking and card teller banking, non-existence of camera such as CCTV at e-banking transaction terminals, absence or inadequate of system base solution to trace and to report suspicious transactions and compromised accounts, lack of compliance to know-your-customer and best practice procedures of e-banking management, no segregation of transaction limits, failure of incorporating string validation test of security, ineffective encryption key management, inadequate control to restricted environment and availability of ex-staff with active login pin to e-banking management system database.

Equally, Odediran (2014) the findings in the study titled "holistic approach to electronic channels fraud management" shown that, the factors that influence the rising cases of electronic banking frauds in Nigeria are Ignorance of cardholders on card usage security, Inadequate monitoring of electronic payment terminals and lack of adequate management of electronic bank production services. Gates and Jacob (2009) have pointed that the factor contributes to increase of e-banking fraud is the mismanagement of technology in the banking industry which comprises theuse of technology for illegal activities, sharing of confidential data, banking access for over-payments to sellers. European Central Bank (2014) in the survey of cards fraud, further elucidated that the contemporary mobile devices with their operating system were not intentionally produced with the security of financial payment, the transmission of personal data and sensitive payment using radio technology leaks mobile payment to risks. Banking services and other financial industries experience losses annually through fraud incidences such as internet banking frauds, cheques and cards frauds (Adams, 2010). Therefore, these signify that fraudsters are exploiting electronic banking channels.

Moreover, Brunner, Decressin, Hardy and Kudela (2004) in their survey found that the location of Automated Teller Machine (ATM) is a high determining factor for fraud

perpetrating at Automated Teller Machine point. From the study, above 75% of the respondents confirmed that the location of ATMs in isolated places without surveillance security such as Closed-Circuit Television (CCTV), Video Surveillance and Security officer subsidise to the fraud occurrence at ATM point. Therefore, ATM within the bank premises is more secured and, it is noticeable that the location of Automated Teller Machine in attractive environment or location does not support it prone for fraud.

Correspondingly, Diebold (2002) reported that the significant form of Automated Teller Machine (ATM) fraud is personal identification number or information (PIN) theft which is performed through several means; shoulder surfing, skimming, camera, key pad recorder and other related means. This study explicates that the major type of perpetrating fraud during the ATM is PIN theft which is commonly happening when there is overcrowding of the users at Automated Teller Machine points. In the same vein, in the investigations of Bernett (2002);Oko and Oruh (2012) found that 24 hours' access to the Automated Teller Machine or point of sales (POS) devices is a "double edge sword" it has both disadvantage and advantage.

Therefore, it is easy to construe that automated teller machine (ATM) fraud incidents occurred mostly in the day time. Also, no dispute, there are some incidences of fraud at night, but most automated teller machine users usually make transactions in the day hence, preventing fraud incidences at night paramount. In addition, Bernett (2002) reported that some banks have no provision for reporting of fraud incidences and there is no enough orientation for the customers on how to operate e-banking devices such as automated teller machine, POS and the similar, neither provision of Fair and Accurate Credits Transactions Act (FACTA) or Automated Teller Machine Manuals for the ATM users.

Also,Roberds (1998) discovered from historical lesson learnt where insufficient security measures caused fraud in retail payment systems. This was backed up by theexample of cloning that led to losses of almost $600 million from the store's value card encryption. Hence there is

need for incessant improvement in safety and security to avert frauds and alleviate the risks suffered by banks, customers and other industries which have resulted to loss of confidence in electronic banking systems (Giles, 2010). Moreover, presently some enhancement development in preventing fraud of electronic banking channels has been experienced. Financial Fraud Action (2011) testified to the actual fraud losses of 10% on credit/debit cards and 24% fraud losses on internet banking lower than the previous years in the UK. This has been accredited to thegrowth and development of electronic banking safety by the use of non-technical and technical approaches. Globally, to protect and safeguard electronic bank accounts and other financial information on their websites, banks spend substantial technology resources in terms of hardware, software, licensing fees, consulting fees and personal hours on providing an infrastructure that will protect electronic banking from fraudsters (FFA, 2016).

Moreover, technological factors, universally, the costs of managing e-banking fraud risk and the number of electronic banking fraud incidents are always increasing due to the sophisticated techniques used by electronic banking criminals (Credit Industry Fraud Avoidance System, CIFAS 2009). Symantec Security Response (2005) found that internationally, on average, 116 e-fraudattacks occurred each day in 2012 through social engineering and customized malware, obtaining unauthorized contact with sensitive information, as against 82 attacks per day in 2011. Likewise, Avinash-Ingole and Thool (2013) agreed that phishing, card skimming, Trojans, spyware and adware, website cloning, cyberstalking, lack of sophisticated antivirus software and weak passwords contribute to the rapid increase of electronic banking fraud. Therefore, the importance of understudy prevention and e-banking fraud cannot be overemphasised.

2.7.2 Non-Technological Factor

Regardless of religion, ethnicity, culture and other factors, some individuals are still being motivated to perpetrate electronic frauds. Irrespective of technology, The American

Institute of Certified Public Accountants (AICPA), and the Association of Certified Fraud Examination (ACFE), (2015) found that the financial pressure to make means is paramount to some individuals, opportunity and rationalization which are the main reasons why fraud happens. In the authors' research found that, 72 percent seek for personal gain while other 40 percent do not recognise their fraudulent actions as a motive for illegal behaviour.

Usman and Shah (2013) discovered that inadequate staff education, customer education and internal control are other areas which need to be addressed to minimise electronic banking fraud. Also, diverse behaviour patterns of customers, electronic banking customers perform different transactions in diverse ways for various purposes and this has become a challenge as it results to variety of genuine customer transactions that would be imitated by fraudsters who change their behaviour regularly to contend with advances in fraud prevention, thus makes it hard to characterize fraud behaviour from genuine behaviour (Wei et al., 2012).

Bank for International Settlements (2012) viewed the cause of electronic banking fraud beyond electronics. Their finding indicates that lack of training, low compliance level and competition are the major reasons for electronic banking frauds and then advised that there is need for money deposit banks in Nigeria to observe the rising graph of electronic banking frauds seriously and make sure that there is no slackness in internal control mechanism.

Choplin and Stark, (2013) in an investigation conducted, finds that bank customers are vulnerable to electronic banking frauds due to lack of education, better awareness and demographics. Abou-Robieh, (2005) reaffirmed this, to prevent payment card fraud, consumer education on personal information protection is essential.

Zimucha, Zanamwe, Chimwayi, Chakwizira, Mapungwana and Maduku (2012) discovered that the causes of electronic banking frauds are insecurity, limited internet access, cultural barriers and poor legislation. Agboola and Salawu (2008) concurred that security is aparamount issue fortheeffectiveness of electronic banking services. El-Guindy (2008) asserted

that most banks are investing on thedevelopment of electronic banking, but not on its security. Although Nigeria financial institutions have invested a lot on information technology infrastructures, most banks and e-businesses in Nigerian still lack cognizance of the significant of security in electronic banking. Therefore, there is a need to look into the issue of protection in electronic banking.

CBN (2010) disclosed that, most electronic banking frauds occur due to inadequate internal control system. Odediran (2014) believed that, the internal fraud which is often committed by bank staff comprises posting or entering of wrong financial information, card and PIN code hacking, account records suppression and collusion with external fraudsters and I do not care attitude managers of branches. Sullivan (2014) opines that financial institutions bear huge losses yearly through electronic frauds such as card fraud, Automated Teller Machine frauds, misused of private passwords and negligent of the customers to their private transaction data and that fraudsters are taking advantages of electronic banking system which therefore demand substantial strategies for better prevention.

Kinkela and Harris (2014) in their study discovered that committing of fraud involve team-up of bank staffs with the security agents in both national and international networking stations and surprisingly their findings revealed that internal staffs that have direct access to the records and personal data of stakeholders and the system of the bank are teaming-up with the fraudsters. Thus, standard procedures of recruitment and adequate training of the staff will contribute enormously in the prevention of electronic banking frauds. Nkemdilio, Bonaventure and Kingsley (2013) find out that perceived job insecurity and inequality had great contribution to employees' fraudulent intent and this is consistent with one of the elements "perceived pressure" in the Fraud Triangle Theory and their finding shows that electronic fraud is beyond technological factor as other means exist that could lead to fraud..

Furthermore, Ganesan and Vivekanandan (2009) warned that risk exist on opening an

electronic bank account via the internet and that cyber protection must be paramount to both internet bank account holders and the bank managements. Chartered Institute of Management Accountants (2008) shared light on the occurrence of electronic banking fraud and concludes such occurs as a result of greed. The author buttresses the point that 63% of fraud cases cited in 2007 were as a result of greed or people's needs and that challenges from gambling and debts also give a room for fraud. Adding, CIMA (2008) opined that temperament and personality also play a vital role in the occurrence of fraud as some good people with good aims and agenda or principles can equally find themselves in the bad company and begin to have a taste for the quick and fast better life, thereby lured into committing frauds. This position of CIMA (2008) validated the element of 'perceived pressure, a motivating factor in Cressey's Fraud Triangle Theory of 1953.

KPMG (2006) asserted that, fraud is certain to occur in an organisation where there is a weak internal control system possibility of preventing exposure to fraud would be low. Both CIMA (2008) and KPMG (2006) positions agreed that fraud can be committed through the concept of reasoning in people as member of staff may take advantage of the electronic platforms to perpetuate fraud by justifying it because they believe mistreatment or low incentive exist in the organization, which is not far fetchedfrom Cressey's fraud triangle theory element of rationalisation.

Shah, Brayanza and Morabito (2007) believed that, bank customer's incompetency, computer illiteracy and negligence in keeping pins and password issued of thee often result in electronic fraud and that educating these customers could prevent occurrence of electronic banking fraud to the minimal. To America Institute Certified Public Accountant and Association of Certified Fraud Examiners (2015) opines that the ineffectiveness of online security, inadequate disciplinary measures by aregulatory body, lack of customer due diligence results in electronic banking frauds and failure to identify beneficial account owners and other

stakeholders like the shareholders, professionals bodies to play their active roles hinders electronic fraud prevention.

Deloitte (2015) in the study of "India Banking Fraud Survey" observed that there is high frequency of electronic fraud occurrence in the banking industry because of absent of oversight by the top management on movement from the present programme, pressure from business to meet unreasonable target and collusion between the external parties and internal parties (employees) and concluded the rising factors for electronic fraud are inadequate customers and staff awareness, inability to integrate data from different sources and few researches in tackling the menace. Some endogenous factors known as the institutional factors that can be traced to the internal environment of the banking industry and these factors were weak internal control and accounting system, weak customers relation procedure, ignoring the know your customers rule (KYC), ineffective information technology system management, poor management of data base system, poor condition of service and salaries, frustrations from personnel strategies and policies, lack of incentive and promotion, unfulfilled promises by the management, irregular call-over, failure to report fraud incident, insufficient infrastructure, poor generic traits and scanty training, Staff enrolment centred on sentiments, and lack of constant re-training (Ojo, 2008; Adeyemo, 2012; Uchenna&Agbo, 2013).

Usman and Shah (2013) stated that frauds in electronic banking services happen as a product of several concessions in security, extending from inadequate internal controls to weak substantiation systems. Hence, there is a need for appraising the factors contributing to the increase in e-banking fraud. Also, CBN(2010) annual report disclosed that almost all the electronic banking frauds that occurred in that year were the result of inadequate internal control systems.

Equally, Calderon and Green (1994) examined 114 actual incidences of corporate frauds issued by the Internal Auditors between 1986 and 1990. The authors concluded that improper

segregation of duties, lack of proper records, and poor internal controls were responsible for almost all fraud incidences. Correspondingly, Jeffords, Marchant and Bridendall (1992) investigated 910 incidences presented by the Internal Auditors between 1981 and 1989 to appraise the exact fraud issues quoted in the Tredway Commission Report. Almost 63% of the 910 incidences were categorized as internal control frauds.

According to Kinkela and Harris (2014), committing of fraud involves team-up of bank staff with security agents in both national and international networking. Surprisingly, their research work revealed that internal staff who have direct access to the records and personal data of stakeholders and the systems of the bank collude with fraudsters.

Deloitte, in the study "India Banking Fraud Survey" (2015) observed that there is a high frequency of online fraud occurrence in the banking industry because of the lack of staff integrity which gives chance to pressure from business and personal to meet unreasonable targets and collusion between the external parties and internal parties (employees). The study of Usman and Shah (2013) "Internet Banking Security" disclosed that 45% of the fraud incidences reported in 2012 included the involvement of managerial and professional staff.

AusCERT (2006), observed that ineffective procedure of fraud reporting also play a role in electronic fraud. Justifying this, AusCERT (2006) reported that in a survey of Australian Computer Crime and Security (ACCS), concluded that the respondents from the organizations that had experience of electronic banking fraud had agreed not to report fraud incidents to anybody outside of their organization as this would cause damage to the company reputation and believed that if all the frauds were reported the fraudsters would not be caught as a result of lack of regulations and records. To Muscat, James and Graycar (2002) organizations have different negative impressions to law enforcement agencies and this has created a chance for fraud occurrence and there is thus a call for prosecution as a tool for fraud prevention as positioned by fraud management lifecycle theory and as guardianship in routine activity theory.

Correspondingly, individual customers may choose not to report the maltreatment they suffer from fraudsters for certain reasons such as unawareness of the impacts of law enforcement agencies and a feeling of taking responsibility for all loses involved (Yar, 2005).

Similarly, Zimucha, Zanamwe, Chimwayi, Chakwizira, Mapungwana, and Maduku (2012);Masocha, Chiliya and Zindiya (2011) discovered that the causes of electronic banking frauds are insecurity, limited internet access, cultural barriers and poor legislation. The study of El-Guindy (2008) supported the view that most banks are investing in the development of electronic banking, but not in its security. Sullivan (2014) argued that financial institutions suffer huge losses yearly through online frauds such as card fraud, automated teller machine frauds, misuse of private passwords and negligence of customers of their private transaction data. This signifies that fraudsters are taking advantage of the electronic banking system which therefore calls substantial strategies for prevention of fraud.

Dorminey, Fleming, Kranacher and Riley, (2010) stated that fraud perpetrators use their position of trust to find an illegal solution to a monetary challenge and believe that nobody will see them, or they are unlikely to be caught. Lister (2007) elucidated opportunity as the "fuel that keeps the fire going", which means that however high the degree of motivation, a fraud perpetrator cannot commit fraud without having the opportunity. Taylor (2011) supported this view with examples of opportunities such as poor management of turnover, improper segregation of duties, and ineffective organizational structure. Soltani (2013) consented that an opportunity allows someone who is a fraudster or trust violator to commit fraud and that there is a link between thepower to conceal fraud and opportunity to commit fraud.

According to Wolfe and Hermanson (2004), opportunity arises as a result of weakness in the internal control of an organization thereby allowing employees to commit fraud. Albrecht, Albrecht and Albrecht (2008) mentioned the lack of audit trail, ineffectiveness of internal controls, weakness of the board of directors, lack of effective anti-fraud disciplinary policy, and

other factors as perceived opportunities to commit fraud. Rae and Subramaniam (2008) also opined that rationalization is an act of justification of trust violation because of lack of integrity or immoral thought in the lives of employees. Albrecht, Albrecht and Albrecht (2008) used examples to describe the rationalization by which some organizations' managers or executives violate the rules and standards of financial statements by increasing the stock price arbitrarily or doctoring financial statements to favour their interest and still believe that it is for the benefit of the company. Given the nature of the Nigerian economy in relation to fraudulent incidents and lawless attitudes, this theory is most useful for discussing the causes of banking frauds in Nigeria. However, the fraud triangle theory is an inadequate model for detecting e-banking fraud. As is said by critics, the rationalization and pressure cannot be observed; also, it is not technologically oriented and is focused solely on the perpetrator.

Exogenous factors are the factors within the external environment of the organisation which are job insecurity, family pressure, group pressure, societal expectations, individual financial burden, individual greediness, national economic recession, poor leadership culture, lack of security, inadequate infrastructure amenities and political instability. Regha (2015) opines many electronic bank customers have become victims of the electronic fraud as aresult of ignorance and unawareness of fraudsters tricks. CIMA (2008) and KPMG (2006) found that the ineffectiveness of online security results in electronic banking fraud and that monetary losses occur as a result of inadequate disciplinary measures by regulatory bodies; lack of customer due diligence (which means failure to identify beneficial account owners and company owners); and other professionals such as accountants, lawyers, police and estate agencies failing to play their roles when a fraudster sets up an unidentified company to hide behind to purchase property (such transactions usually need the services of these professionals). Bhasin (2016) argued that frauds commonly occur in the banking industry when procedural and safeguards controls are insufficient, thus allowing the system to become vulnerable to the fraudsters or perpetrators.

S/N	AUTHORS	COUNTRIES	STATITICAL TOOLS	FINDINGS
1.	Chiezy and Onu (2013)	Nigeria	Multiple regression analysis and pearson product moment correlation	This study reveals that there are poor employment practice and lack of effective employee training usually over-burdened staff ,weak internal control systems, and low compliance levels on the part of Bank Managers, Offi-ces and Clerks. However, technology can play a major part in combating new-age fraud.
2.	Jansen and Leaukfeldt (2016)	Netherland	Semi -structure Interview	The findings reveal that victimizations Malware and phishing attack were marginally influenced by suitable targets.
3.	Hammud, Bizri and El baba (2018)	Lebanon	Structural Equation modelling withSPSS	Findings show that reliability, efficiency and ease of use; responsiveness, communication, security, privacy all have a significant with reliability being the dimension with the strongest impact
4.	Wada and Odulaja (2012)	Nigeria/USA	Social Theory	The findings holds that the combinations of the of a capable guardian with a suitable target and a motivated offender in a convergence of space and time has an influence on the victimization of malware& phishing.
5.	Jamieson, Stephen and Winchester(2007)	Austria	Fraud Management Life Cycle Theory	Findings expose that the improper interrelationship of distinct groups and com ponent of these stages could result to successful control& perfect Management of fraud in the organization.
6.	Hutchings and Hayes (2009)	Australia	Exploratory study Analysis	Findings revealed that probable victims who perform routine activities through online are morevulnerable to

				be defrauded by motivated offenders .
7.	Choo (2011)	Australia	Mixed Method and routine Activity theory	Studies shows that routine activities theory can be applied to mitigate these risks by reducing the opportunities for cybercrime to occur making cyber crime more difficult to commit and also by increasing the risk of detection and punishment associated with committing cyber crime
8.	Pratt , Holtfreter and Reisig (2010)	USA	Regression Model	These findings support routine Analyses Theory (RAT) perspec-tive and provide a theoretically informed direction for situa-tional crime
9.	Karmen (2010)	New York	Regression Techniques	Findings revealed that reporting rate showing that online identity theft associated with personal and physical guardianship and identifying public Internet access and online auction selling as highly risky routine activities.The paper concludes by emphasizing theimportance of studying country-level effects ononline identity theft victimization.
10	William (2015)	United Kingdom	Multi-level Analysis data	The paper adds to the theory of cybercrime and policy debates by: showing that country physical guardianship (e.g. cyber security strategy) moderates the effects of individual physical guardian-ship; introducing a typology of online capable guardianship: passive physical, active personal and avoidance personal guardianship.

Source: Author's Compilation, 2019

2.8.Review of Fraud Prevention Variables

This section review prior literature on dependent variables of technological mechanism and e-banking fraud prevention; customer whistleblowing and e-banking fraud prevention;

surveillance mechanism and e-banking fraud prevention; and staff customer awareness/ education and e-banking fraud prevention.

2.8.1Customer WhistleBlowing and Fraud Prevention

Complaints about banking fraud and scams hit an all-time high in the past financial year, according to the UK's Financial Ombudsman Service, prompting campaigners to claim that financial fraud is spiralling out of control as over 12,000 customer complaints about financial fraud were lodged with the ombudsman in 2018/2019, an increase of 40 per cent on the previous year and more than double the volume received three years previously. Push payment banking scams, where customers are conned into authorising money transfers online, has driven the rise in complaints according to the ombudsman, which described it as one of the fastest-growing types of fraud (Beioley, 2019).

According to Acquisti, Friedman and Telang (2006), the key aspect of most of these e-banking fraud preventive measures is that deposit money banks (DMB) feel pressured to take appropriate actions but these, however, depends on whether customers pay attention to security frauds and if they are willing to hold the banks responsible and that after a breach or an adverse event, experience showed that the confidence of customer on the e-banking system suffers. If anything, researchers argue that repeated disclosures of data breaches or notices of hacking makes consumer immune to these events and they are more likely to ignore them (Experian, 2014).

According to Experian (2014), disclosure and transparency policies implicitly assume that customers of banks are paying attention and are willing to adhere to guidelines as prescribed by their banks in relation to preventing online fraud. In reaction to customer complain and whistleblowing, many banks across the globe now install their own customer service programs online assuming that these programs may alleviate e-banking fraud and they do by rolling out

Internet and mobile-based access to customer accounts whereby they get instant alerts, One-Time Password (OTP) prompt, check balance and prince statements but however while these services are attractive to end users, they also come with significant security risks.

Bhasin (2007) opines that as much as financial institutions, independent organizations and the media communicate to consumers that they should not share confidential data, many people do share their information with close friends and family, giving rise to a number of identity theft cases as these close friends and family members pretend to be the customer and steal from that individual. These are very time-consuming cases to research, but they can present a lower risk to the institution if the case is referred back to the customer to handle in a civil (rather than criminal) manner and it could be devastating to an individual to learn that he or she has been deceived by a close friend or family member, these cases can be especially difficult for victims.

More so, researchers and finance professionals has identify whistleblowers as the most important tool for fraud prevention that can save substantial resources that would go into fraud investigation if whistle-blowers emerge early enough and quite often (ACFE,2016).

The United Nations Convention against Corruption (UNCAC) is a good starting point to support whistleblower protection legislation. Articles 6, 13 and 39 recommend ensuring the existence of an independent body (or bodies) that prevent corruption, which are known to the public and have the capacity to receive anonymous reports. It further recommends, in Article 33, enacting appropriate legislation to provide protection for persons reporting those incidents. Even though the UNCAC targets corruption broadly and not specifically in relation to the banking sector, the mechanisms envisaged in the Convention, if effectively implemented, would benefit informants in that sector e-banking and fraud generally. These measures should be considered as enabling steps to implement the principles expressed in UNCAC and promote a culture where bona fide whistleblowers in the financial industry and in other sectors are safely enabled to come

forward with concerns.

Employees and third parties should be encouraged to report their suspicions of fraud or other irregular activity without fear of reprisal. To encourage reporting, whether anonymous or not, an E-mail or telephone fraud hotline can be implemented to boost whistle blowers confidence.. The existence of such facilities should be well publicized and their roles in preventing and deterring e-banking fraud and information gathered from these blowers should be treated on a confidential basis to reassure whistle blowers, and management should be seen to be fair and just in handling such confidential information (NDIC, 2010).

2.8.2Surveillance Mechanism and Fraud Prevention

Every year, banks suffer millions of dollars in losses from fraudulent activities to usage of online channels. In fact, the American Bankers Association estimates bank online channel services cost the banking industry about $1.9 billion to losses in 2014 alone (America Bankers Association Deposit Account Fraud Survey, 2015). To this end, Peled (2007) opines that video surveillance technology if employed in conjunction with other security measures such as supplementary technology, information sharing with authorities, widespread employee and consumer education can help solve any number of such crimes.

Summer (2016) asserted that video surveillance is helping financial institutions solve electronic banking crimes with video evidence that verifies what took place and it is this fear created by mounting of CCTV, web cameras that have created preventive measure to curb fraud in deposit money banks across cities and surveillance systems with video-based business intelligence go one step further by incorporating ATM and teller transaction data, as well as powerful analytics, to proactively prevent fraud occurrence.

2.8.3Technological mechanism and Fraud Prevention

The phenomenal spread of branches, growth and diversification in business, large-scale computerization and networking, have collectively increased manifold the operational risks faced

by the banks. Unfortunately, it is also true banking industry has to face many types of frauds and scams. These inadequate measures to prevent banking fraud is the primary reason for widespread frauds and technology, an evolving tool which has become a double-edged sword as is both used to perpetuate and prevent frauds (Bhasin, 2016).

As Kumar and Sriganga (2014) stated, by leveraging power of data analysis technology, banks can prevent fraud very soon and reduce the impact of losses and that also new technology now prove to be very helpful to control the fraud risk in banks.

Recently, e-banking transaction has become more complex with the development in the field of information and communication technology, which has changed the nature of bank fraud and fraudulent practices and to this effect, Berney (2008) observed that customers rely heavily on the web for their banking business, which leads to an increase in the number of online transactions. Similarly, Gates and Jacob (2009) and Malphrus (2009) asserted that the internet provides fraudsters with more opportunities to attack customers, who are not physically present on the web to authenticate transactions and this has thrust enormous responsibilities in terms of prescribing and maintaining an effective architecture of internal checks and controls, and optimum use of innovative technology.

According to Wells (2005) banks have more technology and more incentive than ever to combat fraud in electronic banking services but whether they have enough technology and incentive to protect consumers from the headaches of a compromised account, payment card or identity is doubtful. There is no simple way to squash fraud, but by implementing the right mix of technologies and prevention techniques and as such, treasury executives can greatly reduce their organization's risk by exploring these viable tools. It has become an endless game of cat and mouse between banks and cyber-criminals; this virtual arms race across online channels had made banks to deploys a new process or technology to prevent online fraud (Dzomira, 2014).

Undoubtedly, technology can prove helpful in fraud prevention in banks (Bhasin, 2007). As the landscape of fraud continues to shift, business leaders must be aware of trends and predictions that will allow them to implement internal/external controls and systems to help reduce the risk of fraud and keep them from becoming another statistic (Mueller, 2015).

Neural Networks have been extensively put to use in the areas of banking, finance and insurance and such applications of neural networks systems involve knowing about the previous cases of fraud, to make systems learn the various trends, where fraud cases are statistically analysed to derive out relationships among input data and values for certain key parameters in order to understand the various patterns of fraud and gained knowledge of fraud trends is then iteratively taught to feed forward neural networks, which can successfully identify similar fraud cases occurring in the future (Bhasin, 2016).

According to Bhasi (2015) some of the technological innovations, which may be already in use in some banks are: Two dimensional Bar Codes, Data Glyphs, Biometrics, Cheque Image Processing, Data Mining and Data Analytics, et cetera. Given this complicated fraud prevention picture, banks will need to figure out their own patterns of exposure and deploy tools with the best fit. There is no one silver bullet to stop all frauds forever as the pace of new threats is not going to slow down and nobody (no bank, no retailer and no consumer) is ever 100% secured but however, what is needed instead is a combination of checks from a layered approach that banks will have to adopt and consumers will have to accept if they want to utilize electronic banking services and that suggests consumers should expect to see, and might want to welcome, an ongoing stream of new technological solutions that banks will employ to stay a step ahead of electronic banking fraudsters and consequently, banks also have begun to deploy an array of other technologies, some of which are so exotic and sophisticated they might seem like science fiction (Bhasin, 2016).

Another good tool for e-banking fraud prevention is artificial intelligence and it is fair to say that Artificial Intelligence has become quite a buzzword in various fields of business and the financial services industry is no exception (Dmitri, 2017).Many bank institutions are heading in the direction as Narrative Science report has put it that 32% of respondents among banks confirmed using AI technologies such as predictive analytics, recommendation engines, voice recognition and response is a viable tool for preventing online fraud (Dmitri, 2017).

However, as technology advances, we are seeing a distinct proliferation of more complex fraud schemes but at the same time, we are seeing more breakthroughs in the use of technology to detect fraud (Mueller, 2015). While advanced technology serves as a great tool to combat fraud, the issue should be viewed as more than just an IT problem and looked at as a business problem. Remember, the cost of trying to prevent fraud is far less expensive to a business than the cost of fraud committed on a business (Bhasin, 2016).

2.8.4 Control Variable: Staff Customer Awareness/ Education and Fraud Prevention

Several years ago around 70 percent of online banking attacks against banks involved account takeovers. Accounts can be hacked into using stolen identity credentials, or off the back of a phishing campaign where the customer is tricked into entering their login credentials on a fake site. Once the account has been compromised, the fraudster then accesses their digital banking account and commits the fraud. Fraudster may not even commit the fraud online as a step-up authentication may cause customer suspicion. Once in control of the customer's machine, they may manipulate the webpage to show additional funds (easy to do via webpage HTML), instructing the customer to go into branch to move the 'new' money out to account the fraudster can control. The fraudsters will even phone call the customer when in branch to 'coach' them not to alert bank staff (Nathan, 2019).

According to Nathan (2019) if e-banking fraud are evolving, so must the banking industry and the first step to tackle it is through staff and customers education by ensuring all

customers have extensive knowledge on the “dos and donts” when it comes to digital and phone banking. Email alerts reminding customers that their bank would never ask for certain information over the phone, as well as adverts raising awareness on the risks of letting another person access their computer, are but a few options that can be used to ensure customers are protected and well-informed. These preventive fraud techniques are especially effective with some of the most vulnerable people in our society, who tend to struggle with the evolution of e-banking channels (Nathan, 2019).

According Mahdi ,Rezaul and Rahman (2010), the banks have to strengthen awareness programs boost customer confidence internet banking and reduce scams. To Nathan (2019), using the customer education strategy for fraud prevention could be undertaking by the following steps: educate the customers to protect their personal information; that they should not share their login/ identifying information with others, that they should monitor their statements and report any unauthorized activity as soon as possible; that they should never respond to e-mails or text messages that ask for account information even if they appear to be coming from a legitimate source; that they should always be leery of any message that refer them to a website; keep their computer protected by anti-virus software; only use the credentials on secure websites when buying or selling over the internet and if they think their personal computer has been hacked into, take it to a certified computer specialist to have them clean up and should report suspicious activities the customer service desk.

Choplin and Stark (2013) conducted a psychological investigation and found that factors such as education and demographics both had an effect on consumers’ vulnerability. Rizzardi (2008) emphasised the place of customers education in preventing e-banking fraud. By educating customer and employees on the latest fraud scams and schemes, banks can prevent fraud before it starts. To Rossi (2016) banks should help their customers understand common email phishing schemes that are designed to have them unknowingly provide their login credentials or banking

details to fraudsters.

For better cooperation between institution in especially those in the banking system, the central Bank of Nigeria (CBN) in 2014 made it compulsory that all account holders should have a Bank Verification Number (BVN) so as to enable the account holder to have a single identity and also to help the banks in the protection of their customers from fraud(Ekwonwune, Sam-Okeke, Etim&Egwuonwu, 2016). It was this anticipatory synergy that gave birth to the establishment of Nigerian Inter-Bank Settlement System (NIBSS, 2014), a body responsibility for viable relationship amongst banks and other financial institutions. This body as established is responsible for the management of the Bank verification number (BVN), a tool that has bridge both private and the public sector.Transaction on modern technologies security is a complex challenge that requires concerted efforts from all stakeholders in the payment space to be effectively dealt with.

However, out of the various channels of electronic banking, only online banking through phishing, malware and card payment fraud prevention has ever received concerns of the researchers, therefore, there is a need to understudy prevention and e-banking fraud in Nigerian money deposit banks with the use of routine activity theory (RAT) and fraud management lifecycle theory (FMLT).

2.9 Review of Theories

Many theories have been developed to elucidate the nature of fraud. Two theories of criminology and management were adopted as theoretical frameworks to underpinned this study, vis-a-vis the routine activity theory (RAT) and fraud management lifecycle theory (FMLT).

2.9.1 Routine Activity Theory (RAT)

The routine activity theory is a significant theory of environmental criminology and a place-based clarification of fraud theory, where the behavioural forms; the interrelationship of people in the place and in time influence where and when fraud occurs. The theory advocates

that when suitable targets and motivated offenders meet without capable guardians, fraud will probably materialize (Miller, 2013). Equally, the non-appearance of any of these listed three circumstances might be sufficient to prevent a fraud from happening. Positioned within the comprehensive context of environmental criminology, routine activity theory proposes that reducing opportunities for fraudulent activities plays a significant role in minimizing the pervasiveness of fraud (Williams, 2016).

However, routine activity theory is, in a nutshell, an effort to identify fraudulent activities and their methods through clarification of vicissitudes in movements in the fraud rate (Cohen &Felson, 1979). It therefore offers a setting of orientation for material and modified fraud analysis and simplifies the application; implementation of actual practices and policies aimed at changing the essential elements that make the presence of fraud probable, thus averting it (Tillyer& Eck, 2009).

The routine activity approach was introduced in the United States by Cohen and Felson (1979).This approach has proved its helpfulness in accounting and banking for a variation of fraudulent activities (Bradford, 2013). The routine activity theory was developed to examine the vicissitudes in the crime rate after World War II (Kennedy & Forde, 1990; Cohen &Felson, 1979). From the societal perspective, routine activity theory specifies that variations in combined routine activities can generate opportunities for fraud.

Furthermore, from the individual perspective, empirical researchers have emphasized the position of the individual or entity's routine activities in generating fraud opportunities (Fisher, Daigle & Cullen 2010). However, the routine activity theory proves that there is an opportunity for the occurrence of fraudulent activities in a place and time when the motivated offenders come together and there is availability ofsuitable targets with absence of capable guardianship. The proposal of a routine activity theory (proximity and acquaintance to target attractiveness, motivated offender, with absence of capable guardianship) has become the main elucidation of

what brings individuals to fraud or being defrauded (Fisher, Daigle & Cullen 2010).

Moreover, the continued acceptance of the theory in clarifying direct-contact fraud incidence has prompted researchers to adopt the theory to describe opportunities for fraud taking place at a distance (Marcum, Higgins & Ricketts, 2010). The theories have mainly concentrated on fraudsters that meet their targets in a place (Tillyer& Eck, 2009). However, some frauds do not require direct and physical contact at a place. This has encouraged philosophers to determine whether the routine activities approach is restricted to place-based fraud (Tillyer& Eck, 2009).

In addition, the struggle of the first researchers to adapt the routine activity approach to frauds in which fraudsters and their victims do not meet in the same space and time have generated assorted, but inspiring results (Marcum, Higgins & Ricketts 2010; Holt &Bossler, 2009). These studies have concentrated on e-banking fraud, such as computer virus contagion and phishing harassment, and suggest that more studies are required for categorizing cyber routine activities that possibly place cyber operators at higher risks of diverse cyber fraud and adapting the theories to describe distance-based fraud. The current research work discourses both phenomena through appraising e-banking fraud, prevention and detection from a routine activities perspective.

The context of e-banking fraud, routine activity theory (RAT) is an environmental theory, a time-and-place-based elucidation of crime, where connection of individuals and behavioural patterns of a place and time influence where and when frauds occur (Williams, 2016). The routine activity theory suggests that there is likelihood of fraud when there is the absence of a capable guardian and the availability of attractive targets and motivated offenders (Marcum, Higgins & Ricketts, 2010). Conversely, the absence of one of these elements might be able to stop e-fraud from occurring. Therefore, this theory is adopted by this study.

In this case, routine activity measures a diversity of hypothetical fraud environments,

such as places and time spent on the internet. The following two routine activities are related to online identity fraud, which is classified into activities and locations of internet access that measure a variety of cyber activities and location access. The first group is cyber activities such as purchasing, banking, auction, selling, email and social networking while the second group is location of internet access, which includes bank, home, public, university, mobile, café and work; some locations are more dangerous than others, such as computers in public places and cafes that have many users, which can increase virus infection (Wilcox, Madensen&Tillyer, 2007).

However, if these approaches of internet activities remain unguarded, this will probably uncover attractive internet targets to motivate electronic fraudsters.

2.9.2 The Fraud Management Lifecycle Theory

The fraud management lifecycle is the proactive use of prevention, deterrence, investigation, policy, analysis, detection, mitigation and prosecution of the fraudsters (Wilhelm, 2004). The fraud management lifecycle theory is a network lifecycle where each node or stage in the lifecycle is a combined entity that is formed of interrelated and interdependent actions, operations and functions (Albrecht, Albrecht & Albrecht, 2008).

The provision of this theory with its components will be adopted in the prevention and e-bank fraud in Nigerian money deposit banks. The adoption of this theory results from its methodical approach for combating frauds. In the first place, this theory creates an environment that deters people from perpetrating both online and offline frauds; it embraces the strategies to avoid frauds from happening.Moreover, Iminza, Gikiri and Kiragu (2015), in their study Operational Governance and Occupational Fraud in Commercial Banks in Kenya: A Positivist Approach proved that the interconnections of the stages in the fraud management network are the main components of the fraud management life cycle theory. The theory is significant; as it clearly illustrates the stages of fraud management in a chronological manner and demonstrates

what institutional procedures and practices should be installed in place for all kinds of frauds to be perfectly and effectively controlled. Furthermore, the theory assumes legal, uniform cultural and technological uses in the prevention of fraud. Therefore, an operation of the theory begins with an explanation of the life cycle platforms and devoid of this consideration, fraud-managing professionals are not likely to relate efficiently with one another both within and without of the organization (Njenga&Osiemo, 2013).

The fraud management life cycle theory posits that the proper interrelationship of diverse groups and components of these stages will result in successful control and perfect management of fraud in the organizations. Therefore, Wilhelm (2004) related the fraud management lifecycle with the need for the management to be responsible for reducing fraud chances and proactive in eliminating fraud opportunities; measuring and identifying fraud; and implementing and monitoring internal control, proper preventive, and other deterrent measures.

Wilhelm (2004) describes the fraud management lifecycle as the accurate interconnectivity of stages of activities such as prosecution, investigation, policy, analysis, mitigation, detection, prevention and deterrence both internal and external to the business environment, to enhance an environment and culture that elevates ethical behaviour and promotion. The operation of the management of the Fraud Management Lifecycle begins with elucidations of its components and one can equitably describe the several life cycle platforms as numerous disciplines in fraud management. The theory is consequently a component in lifestyle; that is, a combined entity of interconnected, co-dependent, and self-governing functions, activities, operations and actions(Wilhelm, 2004).

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter expounds the methodology and methods that were adopted for this study. The chapter extensively explainedthe research design, population and sampling of the study, research instrument; data collection, model specification and testing procedures. It takes a review on data preparation and analysis.

3.2 Research Design

The study employed the use of a cross-sectional research design technique; vis-a-viz quantitative research methods. The choice of the research design is because data for the study was collected from various respondents at a particular point in time, a reliable method that the researcher believes will create a boost for the study as aone-on-one meeting with the customers (respondents) who are the victims of these frauds combine quantitative with coding and analysis of data is by no means a good research strategy.

For better model structure, analysis and results, the study introduced Staff/Customer Awareness and Education (SCAE) as control variable.

3.3 Population of the Study

The Nigerian deposit money banks, comprises 22 banks with 3979 branches all over the country. It holds 78% of the capital reserves, total net assets and share over 83% of total profitability of the entire banking sector (CBN Bank Supervision Report, 2018).

Owing to the inter-connectivity nature of e-banking transactions and operations amongst the banks, targeted customers for our population is 440 (22 MDBs multiplied by 20 customers each)

On this ground, Omotayo, and Kulatunga (2015) observed that, in most cases, as administering thequestionnaire to the entire population is very cumbersome, as there exist inadequate time, limited access, insufficient funds and other perceived drawbacks. Thus, for these reasons, it will be very easy to survey a subgroup of the population, which means a "sample".

3.4 Sampling Size

In deciding the sample size to be used, the work takes cognizance of the fact that the sample size will be a good representation of the whole population. To determine the sample size, the Taro Yamane (1967) method is employed.

This is designated by the formulae:

$$n = \frac{N}{1 + N(e)^2}$$

Where: n =the sample size

N = total population size

1 = constant

E = error limit (5% Error and 95% level of confidence).

$$n = \frac{440}{1 + 440(0.05)^2}$$

$$n = \frac{440}{1 + 440(0.0025)}$$

$$n = \frac{440}{1 + 1.1}$$

$$n = \frac{440}{2}$$

$$n = 220$$

3.4.1 Sampling Techniques

Sampling for this study is 220 customers of the 22 money deposits banks (MDBs) in Nigeria while targeted place for survey is theheadquartersof these banks in Lagos and Abuja. These 220respondents from the 22 banks were selected as a unit of the population, using the

Taro Yamani (1967)method.

In the course of the distribution, and to ensure that the sampled banks which ultimately constituted the population, were represented 10 copies of the questionnaire were distributed to the banks, filled and returned.

3.5 Methods of Data collection

Primary data were collected through the means of questionnaires and thequestionnaires survey strategy was employedfor the study.

The study seeks for permission through telephone calls and letter of consent sent to the selected banks as thisallowedaccess into the headquarters of the selected banks located in both Lagos and Abuja.

3.6 Research Instrument

The questionnaires is in Section A and Section B. Section A labelled 'Demographic Data' with 6 Questions while Section B examines e-banking system and fraud prevention in Nigerian money deposit banks with an in-depth look into the dependent and independent variables with a total of 35 questions.

Specifically, the Likert scale is in the following format: Strongly Agreed 5, Agreed 4, Undecided 3, Disagreed 2, Strongly Disagreed 1. However, there are different names given to the varying states depending on the kind of rating individual researcher preferred (Brown, 2014). For the benefit of this study, the researcher maintained the original format by assigning scores from 5 to 1 from positive to undecided options. Thus the five-point Likert scale is adopted for this study,which bears the following rates: Strongly Agreed 5, Agreed 4, Undecided 3, Disagreed 2,Strongly Disagreed 1

3.7 Reliability and Validity of Instrument

A sample of 100 customers was selected from these 22 money deposit banks in Nigeria as pilot-test in order to have a reliable instrument for the study. Upon their return, the Cronbach

alpha test was undertaken and this allowed for some adjustments of the questionnaire. The Cronbach's alpha has a threshold value of 0.7.

3.8 Model Specification

This study adoptedquantitative research methods with the aid of descriptive statistics and regression analysis, hence a ground upon which a model must be fashioned for our study.

Previous study;Enofe, Abilogun, Omolorun and Elaiho (2017) regarding Bank Fraud and Preventive Measures in Nigeria: An Empirical Reviewadopted an econometric model to test the hypothesized relations. In their study, below model was formulated:

$BFPt= \beta_0+ \beta_1ICSt+ \beta_2CGt+ \beta_3CBEt+ ut$

Where: BFP = Banks Fraud Prevention

ICS = Internal Control System

CG = Corporate Governance

CBE = Compliance with Banking Ethics

u= Error term.

β0= Intercept/Constant,

β1, β2, β3 are slope/coefficient,

Apriori signs are: β1, β2, β3,>0

Thereforethis study adopts the model stated above with modification and addition of control variable in order to produce a reliable and dependable result in arriving at an achievable research;our model is specified in functional and econometric form as:

FP =f(EBS, SCAE) ..... (1)

The above model is stated in its functional form, however in order to take into account its stochastic aspect of the model it is therefore stated in its econometric form as:

FP= f (CWB, SUVMEC, TECMEC, SCAE)

$FP = \beta_0 + \beta_1 CWB + \beta_2 SUVMEC + \beta_3 TECMEC + \beta_4 SCAE + Ɛ$

Where:

FP = Fraud prevention

CWB =Customer whistle-blowing

SUVM= Surveillance mechanisms

TECM =Technological mechanisms

SCAE = Staff- customer awareness and education (SCAE is a control variable)

β_0 is the constant, and Ɛ is the error term

Apriori Expectation: $\beta_1, \beta_2, \beta_3, \beta_{4,>O}$

3.9Data Analysis Method

This study employed descriptive statistics, demographic analysis of respondents, test of heteroskedasticity, test of misspecification, Cronbach alpha test and regression analysisvis a avis t-test, r-square reset, Durbin Watson test, etcetera.

3.10 Measurement of Variables

A 5-point Likert scale ranging from 1 (Strongly disagree) to 5 (Strongly agree) was adopted for the study.The 5-point Likert scales are rating scales widely used for asking respondents' opinions and attitudes are utilized to ask the individual investors to evaluate the degrees of their agreement with the impacts of behavioural factors on their investment decision. The information obtainedwas coded and subjected tovarious statistical packages namely: SPSS and Eviews 8.0.

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

4.1 Introduction

The focus of this section is on the data presentation and analysis based on the tentative statement that was made about the population parameters. The research survey included quantitative questionnaire which comprises the administration of 220 for banks' customers. The questionnaire included the 6 demographic information of the respondents and 35 likert structured questions covering independent, dependent variable and the control variable.

This chapter demonstrates the analysis of the data gathered, starting withthepresentation of the descriptive measurement, which commenced with the demographic attributes of the respondents andthe performance of the statistical analyses using E-View and SPSS combine with the interpretation of the outcome of results and test.

4.2 Presentation of Data

Table1: Administration and Report ofQuestionnaires

BANKS COPIES OF	COPIES OF QUESTIONNAIRE DISTRIBUTED	COPIES OF QUESTIONNAIRE RETURNED	QUESTIONNAIRES USED
First Bank	10	10	10
Zenith Bank	10	10	8
United Bank for Africa	10	6	6
Eco Bank	10	8	8
Guarantee Trust Bank	10	9	9
Stanbic IBTC	10	8	8
Access Bank	10	9	9
Wema Bank	10	9	9
Fidelity Bank	10	9	9
Unity Bank	10	9	9
Starling Bank	10	6	6
Heritage Bank	10	7	7
Union Bank	10	6	6
Keystone Bank	10	8	8
Polaris Bank	10	6	6
FCMB	10	8	8
CitiBank	10	9	9
Standard Chartered	10	9	9

Providus Bank	10	5	5
Jaiz Bank	10	7	7
Suntrust Bank Nig. Ltd	10	6	5
Globus Bank	10	5	4
	220	**169**	**165**

Author's Survey, 2019.

From Table 1, the summary of the administered copies of thequestionnaire could be seen. As it turned out, 169 of the 220 determined copies of questionnaire were returned while 165 of the returned copies of questionnaire were used for the study. As for the remaining 4, their inability for usage as accounted for inappropriate response of the respondent.

Table 2: Demographic Details of Respondents

VARIABLES	CATEGORIES	FREQUENCY	PERCENTAGE
Gender	Male	39	47.0%
	Female	44	53.0%
	Total	**83**	**100%**
Age	20years - 30years	70	84.4%
	31years – 40years	6	7.2%
	41years – 50years	6	7.2.%
	51years and above	1	1.2%
	Total	**83**	**100%**
Marital Status	Single	62	74.7%
	Married	7	8.4%
	Separated	13	15.7%
	Divorced	1	1.2%
	Total	**83**	**100%**
Educational qualification	OND	12	14.8%
	Bsc/HND	43	51.8%
	MSc/MBA	9	10.8%
	Others	19	22.6%

	Total	**83**	**100%**
Societal Class	Top	18	21.7%
	Middle	32	38.6%
	Low	33	39.7%
	Total	**83**	**100%**
Type of Account	Savings	12	14.5
	Current	43	51.8
	Fixed Deposit	9	10.8
	Others	19	22.9
	Total	**83**	**100**

Source: Authors' fieldwork 2019

With respect to the gender of the respondents' in Table 2, it was observed that 47% of the respondentswere male while the remaining 53% were female respondents. A further look at the next demographic element age of respondents shows that 84.4% of the respondents were between 20-30years,7.2% of the respondents were found to be between the age of 31- 40 and 7.2% of the respondents were found to be between the age 41-50 while the remaining 1.2% were found to be above 51years above. An examination of the third demographic variable which is the marital status of the respondentsrevealed that 74.4% of the respondents were single, 8.4% of them were married, 15.7% of the respondents were separated; while, 1.2% were divorced.

On the fourth demographic variable which is educational qualification; it was observed that 14.8% of the respondents were OND holders, 51.8% possessedB.Sc/HND, 10.8% were M.Sc/MBA degree holders, while the remaining 22.6% of the respondents are holders of other certificates. With respect to Societal Class, it was observed that 21.7% of the respondents were High Class, 38.6% were Middle Class while the remaining 39.7% were Low Class. As for the

their type of account, it was observed that 14.5% operateSAVINGS, 51.8% wereCURRENT Holders, 10.8% operateFIXED DEPOSIT, and the remaining 22.9% operate other type of accounts.

4.3 Analysis and Interpretation of Results

Table 3:DescriptiveStatistics

	FP	CWB	SUVMEC	TECMEC	SCAE
Mean	2.751807	2.351807	2.698795	2.537349	2.737349
Median	2.600000	2.200000	2.600000	2.400000	2.800000
Maximum	4.200000	4.400000	4.400000	4.600000	4.400000
Minimum	0.400000	0.000000	0.000000	0.000000	0.000000
Std. Dev.	0.769282	0.938390	0.957830	0.792605	0.955563
Skewness	-0.134501	0.268228	-0.314555	-0.195384	-0.413569
Kurtosis	3.266623	2.934740	3.683671	4.375515	3.770098
Jarque-Bera	0.496096	1.009982	2.985185	7.071398	4.417015
Probability	0.780323	0.603511	0.224789	0.029138	0.109864

Source:E-View,8.0

FP =Fraud Prevention
CWB = Customer whistle blowing
SUVMEC= Surveillance mechanism
TECMEC= Technological mechanism
SCAE = Staff-Customer awareness and education (Control variable)

Table 3indicate the descriptive statistic of variables. From the Table 3 results, FP has 2.751807 with maximum valueof 4.2 and aminimum value of 0.40. It had a standard deviation of 0.769282 which is a bit far from the mean value 2.751807. FP was negatively skewed with skewness value of -0.134.SCAE had the highest mean value of 2.800000 while CWB had the highest skewness. Also, the Jacque Bera statistics which measures the normality of the distribution stood at a value of 0.49. An examination of all other explanatory variable showed

that they are all normally distributed when tested at the 5% level of significance.

A major problem associated with primary data is the issue of validity and the extent of reliability that can be placed on the research instrument. Thus, to check this weakness and ensure the robustness of our findings, the Cronbach's Alpha test was used to determine the internal consistency of measurement scales and reliability of the research instrument and the test result is placed below:

Table 4:Cronbach's Alpha co-efficient

Cronbach's alpha	Internal consistency
$\alpha \geq 0.9$	Excellent (High-Stakes testing)
$0.7 \leq \alpha < 0.9$	Good (Low-Stakes testing)
$0.6 \leq \alpha < 0.7$	Acceptable
$0.5 \leq \alpha < 0.6$	Poor
$\alpha < 0.5$	Unacceptable

Source: Cronbach (1951)

The Cronbach Alpha coefficient of scale stipulates a standard of above 0.6 for acceptability. The result of the reliability test is given below:

Reliability Statistics

Cronbach's Alpha	N of Items
.836	35

Source: Spss,24.0

The result from Table 4, showed that the Cronbach stood at 0.836, which is above 0.6 and therefore indicates an internal consistency. Going by this resultthere exists a robust and a reliable internally consistent score variance.

Table 5: Test for Heteroskedasticity

Heteroskedasticity Test: Breusch-Pagan-Godfrey

F-statistic	0.246926	Prob. F(4,77)	0.9107
Obs*R-squared	1.038518	Prob. Chi-Square(4)	0.9039
Scaled explained SS	0.895407	Prob. Chi-Square(4)	0.9252

Author's compilation

From thetable 5; result of the test for heteroskedasticity showed that R-squared value stood at 1.038518 with an associate probability value of 0.9and therefore indicates that the presence of heteroskedasticity does not exist in our regression model.

Table 6: Test for Misspecification

Ramsey RESET Test

Equation: UNTITLED

Specification: E_BANK CWB SUVMEC TECMEC SCAE C AR(1)

Omitted Variables: Squares of fitted values

	Value	Df	Probability
t-statistic	1.159170	75	0.2501
F-statistic	1.343676	(1, 75)	0.2501
Likelihood ratio	1.456081	1	0.2276

Source: Eviews,8.0

From table 6: result of various specification errors such as omitted variables incorrect functional form and thecorrelation between independent variables and error term lead to the performance of this test, the test is performed to determine whether there were specification errors. The result revealed that high probability values that were greater than 0.05 meaning that there was no significant evidence of miss specification.

Table 7: Regression Result

Dependent Variable: FP

Method: Least Squares

Date: 11/15/19 Time: 11:04

Sample (adjusted): 2 83

Included observations: 82 after adjustments

Convergence achieved after 5 iterations

White heteroskedasticity-consistent standard errors & covariance

Variable	Coefficient	Std. Error	t-Statistic	Prob.
CWB	0.428506	0.123847	3.459970	0.0009
SUVMEC	0.444949	0.121308	3.667917	0.0005
TECMEC	-0.100217	0.156635	-0.639812	0.5242
SCAE	-0.219582	0.081012	-2.710503	0.0083
C	1.400116	0.246097	5.689280	0.0000
AR(1)	0.000352	0.119217	0.002952	0.9977

R-squared	0.468306	Mean dependent var	2.753659
Adjusted R-squared	0.433326	S.D. dependent var	0.773830
S.E. of regression	0.582522	Akaike info criterion	1.827456
Sum squared resid	25.78922	Schwarz criterion	2.003557
Log likelihood	-68.92569	Hannan-Quinn criter.	1.898158
F-statistic	13.38789	Durbin-Watson stat	1.984692
Prob(F-statistic)	0.000000	Wald F-statistic	33.94307
Prob(Wald F-statistic)	0.000000		

Inverted AR Roots	.00

Source: E-views,8.0

From Table 7; the regression analysis carried out, the result shows that our model is fit as the F-statistic stood at 13.38789 as it is significant above 1%, while the Durbin Watson stood at 1.984692. From table7, using the ordinary least squares regression analysis technique our independent variables at 5% significant level can be interpreted thus:

Firstly, CWB has a positive t-value of 3.459970, meaning CWB is strongly and positively

impacting on FP. Therefore, this outcome provided a ground for the rejection of our Hypothesis $Ho_1$of the study that states that: Customer whistleblowing has no significant relationship on fraud prevention in Nigeria money deposit banks.

Moreso, the regression result indicates that SUVMEC possessed a positive t-value of 3.667917 which implies that SUVMEC is positively impacting FP and therefore provide ground for rejecting our hypothesis Ho_2 which state: Surveillance mechanism has no significant relationship on fraud prevention in Nigerian money deposit banks.

In addition, the result also showed that TECMEC has a t-value of -0.639812,meaning that TECMEC is negatively impacting on FP. Hence, the ground for the acceptance of our hypothesis $Ho_3$of the study: Technological mechanism has no significant relationship on fraud prevention in Nigerian money deposit bank.

With respect to the summary statistics, it was observed that the coefficient of determination depicted as R^2 stood at a value of 0.46 and this, therefore, implies that the model accounts for 46% of the systematic variation exhibited by the dependent variable, while the remaining 54% left on accounted for is been captured by the stochastic error term. The F-statistics which measures the overall significance of the model stood at a value of 13.3 with an associated probability value of 0.00 thereby indicating that the model is jointly statistically significant when tested at the 5% level of significance.

The Durbin Watson statistics which measure the presence of autocorrelation in the model stood at a value of 1.98 therefore indicating that thepresence of spatial correlation does not exist in the model.

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

The overall objective of the study was to examine the relationship between E-banking system and fraud prevention in Nigeria. The chapter concludes on the findings of the study and highlights salient policy recommendations.

5.2 Summary of Findings

The emphasis of the discussion was based on these research questions:What effectdo technological mechanisms have on fraud prevention in Nigeriandeposit money banks?Does customer whistleblowing impact on fraud prevention in Nigeriandeposit money banks?What is the relationship between surveillance mechanisms and fraud prevention in Nigeriandeposit money banks?

Each of these research questions was discussed from quantitative analyses carried out and were also supported by the literature reviewed.

Firstly, it was observed that customer whistle blowing has a strong and positive impact on fraud prevention. Our findings provided a ground for rejecting of our Hypothesis $Ho_1$of the study that states that: Customer whistleblowing has no significant relationship on fraud prevention in Nigeria money deposit banks.

Secondly, our findings revealed that Surveillance mechanism possessed a positive impact on fraud prevention, a ground upon which our hypothesis Ho_2: Surveillance mechanism has no significant relationship on fraud prevention in Nigerian money deposit banks as rejected.

More, the findings showed that Technological mechanism is negatively impacting on fraud prevention and hypothesis $Ho_3$of the study: Technological mechanism has no significant relationship on fraud prevention in Nigerian money deposit bank should be accepted.

5.3 Implication of Findings

Findings of the study have some salient implications; not only for researchers, but also for policymakers in the Nigerian financial sector; anti-fraud agencies and all stakeholders in the Nigerian money deposit banks. It is crystal clear that the findings of this study will in no doubt enhance academic research, dictate better policy focus, pioneer a viable fraud fighting reference point for anti-fraud agencies and present a bridge upon which all stakeholders of the money deposit banks in Nigeria can synergise.

5.4 Conclusion

E-banking system representsa new age whereby delivering of services is through automated channels to customers and it provides customers withan opportunity to gain access to their accounts, execute transactions, and obtain information on financial products and services through a public or private network.The Nigerian banking sector has become more complex with the arrival of various electronic channels, which has changed the nature of fraud and fraudulent practiceson the face of the money deposit banks.This menace has eaten deep into customers' savings, banks credibility and even their cash flow and the overall Nigeria GDP and image. No doubt, anti-fraud agencies like the EFCC, the Nigeria police, etcetera have put in some effort but these effortshave been defiled on the ground that the e-banking system wears a borderless and remote mask.

While is arguable that technology has responded to the fraudulent activities on electronic channels, it a common fact that this same technology has been exploited by fraudsters to perpetuate this evil; which has branded the electronic banking world like a sword with two edges

with a blessing and a curse.

From theliterature reviewed and findings of this study one would agree that customer whistleblowing, surveillance and technological mechanisms could extremely be exploited by the banks and its stakeholders to prevent these frauds.

In the face of this financial 'Sodom and Gomorrah', what is expected of the Nigerian money deposit bank, the Nigerian financial sector and the global financial world is prevention over detection and investigation; as what is prevented need no cost, time wastage and effort.

5.5Recommendations

The study hasbirthed some salient recommendations for the stakeholders of theNigerian money deposit banks and overall financial sector of the Nigeria economy in order to minimize the incidences of fraud in e-banking channels. It is glaringfrom our study that fraud has become a menace to the Nigerian e-banking system and that fraud prevention mechanisms as discussed possessed the capacity to eliminate or minimisefraud if stakeholderscontinue to assign significant interest, funds and other resources to the advancement of area like customer whistleblowing,surveillance mechanisms, technological mechanisms and staff-Customer awareness/education;

Staff-customer awareness/education has its role to play. Workshops and seminars should not only be for bank staff, but also banks stakeholders particularly customers. These customers should be kept abreast on tricks of fraudsters and how not to fall victim. Furthermore, individual banks should carryout training and retraining for staff on local and international content on e-banking channels as online fraud is borderless and remotely

Implementation of sophisticated surveillance mechanisms for prevention of fraud should be place, particularlyfor the top e-banking fraud types in Nigeria. The Nigeria MDBs should partner local and foreign firms for better deployment of surveillance tools and technicalities in handling this equipment by banks security officers. Also, there should bean establishment of a

centralized fraud database that would provide a common arsenal whereby fraudulent transactions could be flags before customers fall victim.

The Nigerian money deposit banks should take advantage of advancement in technological mechanisms like biometrics verification and authentication, one-time-password for all online transactions especially shopping. Adding to this, the banks should acquire modern and enhance automated teller machines (ATMs), POS, Smart tabs and tokens. For better management of mobile banking on customers, banks should provide antivirus and tracking software for their customers at thepoint of configuring them (personal computers, tabs, mobile phones) on e-banking platforms while securing the channels away from hacker as this will protect individual e-banking customers from the fraudsters using viruses to hijack their account information.

Furthermore, for betterment of preventing fraud in the Nigeria money deposit banks, complaints of customers should be given faster ears so as arrest fraudulent suspicious before any fraud occurs. There should be viable and efficient customer service center both online and off-line manage by dedicated and trusted staff. In addition to these, whistleblowing should be given a priority; solid company's policies should be enacted to protect the identities of whistleblowers so as not to become victims and also MDBs should handsomely place a reward system for these whistle blowers. The use of suggestion and complain box must not be overlooked so as to assist in preventing frauds.

5.6 Recommendations for Further Studies

This study has produced enough information as regardse-banking system and fraud prevention in the Nigerian money deposit banks. However, there exist some aspects that need to be covered for by future research. Few aspects of such area are; expansion of sample size, variables, and consideration fraud across borders as e-banking channels are used remotely.

5.7Contribution to Knowledge

The primary aim of the researcher in this study is to examine the e-banking system and

fraud prevention in Nigeria deposit money banksfrom a new perspective. So far most studies on electronic banking and fraud were focused mainly on detection and investigation. In this study the researcher has tried to shift focus to prevention as what is prevented requires neither detection nor investigation.

For range of researches on issues regarding fraud, theories such the Cressey's 1953 Fraud Triangle and Fraud Diamond by Wolf and Hermanson2004 always take centred stage but this study hinges it theoretical review on the Routine Activity (RAT) and the Fraud Management Life Cycle theories, a ground that will give fraud researchers and forensic student a new theoretical outlook.

Contribution from this study is wide and immense in scope as responses to the survey conducted validate stipulated hypotheses, hence the following contributions:

1. The study provides a framework for the discussion on the subject of e-banking system and fraud prevention. It helps to correct earlier perception that fighting fraud begins from detection as what is prevented save time, stress and money.
2. The study revealed that across different bank online channels, customers is confronted with fraudulent issues and that new approach as customer whistle blowing, surveillance and technological mechanisms are required in the present situation to forestall frauds in Nigeria e-banking system.
3. The study highlight the need for further studies on fraud in e-banking system as the nature of such fraud is borderless therefore requires data beyond Nigeria.

References

Abdullahi, R., Mansor, M., &Nuhu, S. (2015). Fraud triangle theory and fraud diamond theory: Understanding the convergent and divergent for future research. *European Journal of Business and Management, 7(28),* 30-37.

Abou-Robieh, M. (2005).*A study of e-banking security perceptions and customer satisfaction Issue*(D.B.A).Retrievedfrom http://search.proquest.com/docview/305340121?accountid=10472

Abu-Shanab, E., & Pearson, J. M., Setterstrom. U. (2019). Internet banking in Jordan: An Arabic instrument validation process.*International Arab Journal of .Information and Technology, 6*(3), 235-244.

Abu-Shanab, E., &Matalqa, S. (2015). Security and fraud issues of E-banking.*International Journal of Computer Networks and Applications (IJCNA), 2(4),*179-187.

Adeniyi, O. M. (2006). *Bank credit and economic development in Nigeria: A case study of deposit money banks*. Jos: University of Jos.

Adams, R. (2010). Prevent, protect, pursue-a paradigm for preventing fraud. *Computer Fraud & Security, 2(7),* 5-11

Adedipe,A. A. (2016).Nigerian internetfraud:Policy/Law changes that can improve effectiveness, *5(7),* 33- 54

Adeniji, A. A. (2004). *Auditing and investigations*. Lagos: EL-Toda Ventures Limited.

Adetiloye, K. A., Olokoyo, F.O., &Taiwo, J. N. (2016). Fraud, prevention and internal control in the Nigerian banking system. *International Journal of Economics and Financial Issues, 6*(3), 1172-1179.

Adewumi, O. (1986). Fraud in banks: An overview. *In Frauds in Banks Chartered Institute of Bankers, Nigeria. 5 (2)*, 17-22.

Adeyemo, K. A. (2012). Fraud in Nigerian banks: Nature, deep seated causes, aftermaths and probable remedies. *Mediterranean Journal of Social Sciences, 3*(2), 279-289.

Acquisti,A.,Friedman,A. &Telang, R.(2006). Is there a cost to privacy breaches? An event study in proceedings of the international conference of information systems (ICIS),

from:http://www.semanticscholars.org/paper/is-there-a-cost-to-privacy-breaches-An-Event –Study.

Agboola, A. A. &Salawu, R. O. (2008).Optimizing the use of information and communication technology (ICT) in Nigerian banks. *Journal of Internet Banking and Commerce, 13*(1), 1-15.

Agwu, E. (2012). A qualitative study of the problems and prospects of online banking in developing economies - case of Nigeria.*Journal of Internet Banking and Commerce, 17*(3), 1-20.

Agwu, M. E. (2014). Reputational Risk Impact of Internal Frauds on Bank Customers in Nigeria. *International Journal of Development and Management Review, 9*(1), 175-192.

Aibieyi .S. (2007). Anti-corruption strategies and development in Nigeria: A case study of the independent corrupt practices commission (ICPC) and economic and financial corruption commission (EFCC). *A Journal of Contemporary Research, 4 (7),*212-234.

Akindele, R. I. (2011). Fraud as a negative catalyst in the Nigerian banking industry. *Journalof Emerging Trends in Economics and Management Sciences, 2*(5), 357-363.

Alao, A. A. (2016). Analysis of fraud in banks: Evidence from Nigeria. *International Journal of Innovative Finance and Economics Research, 4*(2), 16-25.

Albrecht, W. S., Albrecht, C., & Albrecht, C. C. (2008). Current trends in fraud and its detection: A global perspective. .*Information Security Journal, 1(7)*, 2-12.

Allen,F., McAndrew, J. & Strahan , P. (2001). E-Finance: An introduction. *Financial Institution Centre. Wharton University,* Philadelphia,*7(2*), 01-36.

American Bankers Association (2015).Deposit Account Fraud Survey, 2014. *ABA Banking Journal*. Retrieved from:https://www.aba.com/news-research/banking-journal

ASSOCHAM. (2015). *Current fraud trends in the financial sector, joint study ofassociated chambers of commerce and industry of India*. New Delhi: PWC. Retrieved from www.pwc/current-fraud-treand.

Association of Certified Fraud Examiners. (2010). *Report to the nation on occupational fraud*Austin, TX: ACFE.

Association of Certified Fraud Examiner (2015). ACFE report to the nation on occupational fraud and abuse. Texas: *Technical Report*.

Association of Certified Fraud Examiner (2016): Report to the nations on occupational fraud andabuse: 2010 Global fraudstudy. Retrieved from:http://www.acfe.com/rttn/rttn-2010.pdf

Ata, H.A., &Seyrek, I. H. (2009). The use of data mining techniques in detecting fraudulent financial statements: An application on manufacturing firms. *The Journal of Economics*

and Administrative Sciences, 14(2), 157-170.

AusCERT.(2006). *Australian 2006 computer crime and security survey*. Brisbane:AusCERT.

Avinash-Ingle, O.&Thool, R. C. (2013). Credit card fraud detection using hidden Markov model and its performance. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(6), 111-120.

Bank for International Settlement (2012). The 2011 skills for life survey: A survey of literacy,numeracy and ICT levels in England. *Department of Business Innovation and Skills, 34(9),* 223-230

Bartholomew, D. (2008). The rhythm of identity management.*Baseline, 81 (3)*, 38-40.

Bartlett, M. S. (1950). Tests of significance in factor analysis.*British Journal ofStatistical Psychology,3*(2), 77-85.

Basel(1998).Framework for internal control system in banking organisations. Basel: Basel committee.

Basle Committee on Banking Supervision (1998) Risk management for electronic banking and electronic money activities, Basle

Beghdad,R.(2008).Criticalstudyofneuralnetworksindetectingintrusions.*Computers & Security, 27*(6),168-175.

Beioley, K (2019). Banking fraud complaints hit 'all-time high. *Financial Times*, May. Retrieved from: https://www.ft.com/content/93f14958-7663-11e9-bbad-7c18c0ea0201

Bernard, H. R. (Ed.). (2006). *Research methods in anthropology*. Lanham: MD-Altamira Press.

Bernett,C.(2002).Themeasurementofwhite-collarcrime using uniform crime reporting (UCR) data.*United StatesDepartment of Justice, Federal Bureau of Investigation, Criminal Justice Information Services 22(9), 32-56.*

Berney, L. (2008), For online merchants, fraud prevention can be a balancing act, *Cards & Payments*, *21(2),* 22-7.

Bhasin, M.L. (2007a). Forensic Accounting: A New Paradigm for Niche Consulting, *The Chartered Accounting Journal*, *7(9),*1000-1010.

Bhasin, M.L. (2007b). Mitigating Cyber Threats to the Banking Industry, *The Chartered Accountant,9 (3*),1618- 1624.

Bhasin, M. L. (2015). Menace of Frauds in the Indian Banking Industry: An Empirical StudyAustralian.*Journal of Business and Management Research,* 4(2), 21-33.

Bhasin, M.L. (2016a), Integration of Technology to Combat Bank Frauds: Experience of a Developing Country.*Wulfenia Journal*, *23(2),* 201-233.

Bhasin, M. L. (2016b). Role of technology in combating bank frauds: Perspectives and prospects. *International Review of Social Sciences, 4(1),* 21-37.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009).Biometric authentication - A review. *International Journal of e- Service, Science and Technology, 2(3),* 77-89.

Blass, A. A., &Oved, Y. (2003).Financing R&D in mature companies: An empirical analysis. *Economics of Innovation and New Technology, 12(5),* 42-58.

Boleigha, P. (2014). Tackling emerging security issues with cyber intelligence in *e-Fraud: fighting the battle, winning the war : Nigeria Electronic Fraud Forum(NeFF),*Annual Reports. 10-11

Boniface, C. (1991). Fraud in the banking industry.*TheNigerian banker,* Oct.-Dec. 22&23. CIBN press.

Bradford, W. R. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50(2),* 2-16.

Brar, T. P. S., Sharma, D., &Khurmi, S.S. (2012).Vulnerabilities in e-banking : A study of various security aspects in e-banking. *International Journal of Computing & Business Research 4(5),* 1-14.

Broadman, H. G., &Isik, G. (2007).*Africa's silk road: China and India's new economic frontier.* Washington: DC: World Bank.

Brown, T. A. (2014). *Confirmatory factor analysis for applied research. Uk:*Guilford Publications.

Brunner, A. D., Decressin, J. W., Hardy, D. C., &Kudela, B. (2004). *Germany's three-Pillarbanking system: Cross-country perspectives in Europe,*International Monetary Fund.

Cahill, E. (2006). Audit committee and internal audit effectiveness in a multinational bank subsidiary: A case study. *Journal of Banking Regulation, 7(*2), 160-179.

Calderon, T., & Green, B. P. (1994). Internal fraud leaves its mark: Here's how to spot, trace and prevent it. *National Public Accountant, 39*(2), 17-20.

Central Bank of Nigeria. (2010). Economic report for the first half of 2002.*Abuja: Central Bank of Nigeria*

CBN Bank Supervision Report. (2018). Financial institutions under the supervisory purview of CBN: Deposit money banks, Retrieved fromhttps://www.cbn.gov.ng/supervision/AllFinInstitutions.asp.

Chanson, S.T.,& Cheung, T.W.(2001). Design and implementation of a PKI-based end- to-endsecure infrastructure for mobile e-commerce. *World Wide Web, 4(4),* 235- 253.

Chartered Institute of Management Accountants (2008). Fraud risk management: A guide togood practice. *Chartered Institute of Management Accountants,7(2),*1-80

Chaturvedi, A., &Meena, A. (2016).Analyzing the impacts of phishing and vishing attacks in Internetbanking.*International Journal of Advanced Research in Computer Science and Software Engineering, 6*(3), 16-21.

Chaudhary, K., Yadav, J., &Mallick, B. (2012). A review of fraud detection techniques: Credit card. *International Journal of Computer Applications, 45(1),* 39-44.

Chiezey, U., &Onu, A. C. (2013).Impact of fraud and fraudulent practices on the performance ofbanks in Nigeria.*British Journal of Arts and Social Sciences, 15(1),* 18-34.

Choo, K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731.

Choplin, J. M., & Stark, D. P. (2013).Doomed to fail: A psychological analysis of mortgage disclosures and policy implications. *Banking & Financial Services Policy Report, 32*(10), 11-19.

Choraś, M., Mroczkowski, P. (2007). Web security enhancement based on keystroke dynamics. Paper presented at the *Third International Conference on Web Information Systems and Technologies.*doi:10.5220/0001264903370340.

CIFAS (2009). ***T****he anonymous attacker: A special report on identity fraud and account takeover*. Tavistock Square London: The UK's Fraud Prevention Service.

Cohen, L.E. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608.

Cressey, D. R..(1953). *Other People's money*. Montclair, NJ: Patterson Smith.

Curt's, C. S.(2013). Costa Mesa, United States, Costa Mesa: Experian Information Solutions, Inc. Retrieved from ABI/INFORM Collection Retrieved from https://search.proquest.com/docview/1587783885?accountid=10472.

Daniel, E. (1999) Provision of electronic banking in the UK and the Republic of Ireland, *International Journal of Bank Marketing, 17*(2),72-82.

Darlington, L. (1999). *Banking without boundaries: How the banking industry is transforming itself for the digital age, blueprint for the digital economy.* New York: McGraw Hill.

Deloitte Fraud Survey.(2015).*The Deloitte in India banking fraud survey.*(Report Edition II). Press Trust of India Report April 23.

Diebold, I. (2002). ATM fraud and security: White paper. *New York:*

Dionco-Adetayo, E. (2011). *Guide to business research and thesis writing*. Ibadan, Nigeria: Rasmed Publications Limited.

Dinapoli, T.P. (2006).Standards of Internal Control in New York State Government.

Retrieved from:www.d/newyorkstatecomptroller.htm.

Dmitri. K (2017). Fraud Management: Detection and Prevention in Banking Industry. Retrieved from https://www.elinext.com/blog/fraud-management-detection-and-prevention-in-banking-industry/.

Drigă, I. (2012) Aspects Regarding Internet Banking Services in Romania, *Annals of the University of Petroşani, Economics, .9*(3), 239-248

Drigă, I., &Isac., C. (2014)E-Banking Services - Features, Challenges and Benefits. *Annals of the University of Petroşani, Economics, 14*(1) 33-58.

Dorminey, J. W., Fleming, A. S., Kranacher, M., & Riley, R. A., Jr. (2010). Beyond the fraud triangle. *The CPA Journal, 80*(7), 17-23.

Duffield, G., &Grabosky, P. (2001).The psychology of fraud.*Trends and Issues in Crime and Criminal Justice, 19(9),* 1-6.

Dzomira, S. (2014). Online and electronic fraud prevention & safety tips cognizance in south African banks.*Socio-economical – the Scientific Journal for Theory and Practice of Socio-Economic Development, 4*(8), 527-540.

Eck, J. E., & Clarke, R. V. (2003).Classifying common police problems: A routine activity approach. *Crime Prevention Studies, 16 (4)*, 7-39.

Economic and Financial Crimes Commission, (2004).Establishment Act 2004. Retrieved from https://efccnigeria.org/efcc/index.php/about-efcc/the-establishment-act

Enofe, A.O., Abilogun, T.O.,Omolorun, A.J., &Elaiho, E.M. (2017). Bank fraud preventive measures in Nigeria: An empirical review. *International Journal of Academic Research in Business and Social Sciences 7*(7), 40-51

Ekwonwune, E. N., Sam-Okeke, D. C., Etim, E.O., &Egwuonwu, D.U. (2016). Biometric database-A tool to fight corruption in a developing nation. *International Journal of Innovative Research in Science, Engineering and Technology, 5* (7*),*12048- 12054

El-Guindy, M. N. (2008).Cybercrime in the Middle East Egypt.*SSA Journal, 4(12),* 1-13.

Elovici,Y. (2009). Identity theft computers and behavioural biometrics. *Intelligence and security Informatics international Conference :* doi:10.1109/ISI.2009.5137288

Eskin, E., &Stolfo, S. J. (2007).*System and Methods for Intrusion Detection with Dynamic Window Sizes,55(6),* 38-56.

European Central Bank.(2014).Third report on card fraud. *Third Report on Card Fraud,*

Entrust (2009).Fighting Fraud In Today's Connected World Critical Approaches to Affordable Fraud Detection. Retrieved from: https://www.entrust.com/wp-content/uploads/2013/05/WP_FightingFraud_July09.pdf

Experian (2014).Aftermath of a mega data Breach: consumer sentiment, http://www.experian.com/data-breach/2014-aftermath-studyconsumer-sentiment.

Ewa, U. E., &Udoayang, J. O. (2012). The impact of internal control design on banks' ability to investigate staff fraud, and life style and fraud detection in Nigeria. *International Journal of Research in Economics & Social Sciences. 2* (2), 32-43.

Fadayo, O.M (2018). An examination of e-banking fraud prevention and detection in Nigerianbanks.Retrieved From: *https://www.dora.dmu.ac.uk/xmlui/bitstream/handle/2086/17520/Oluwalami%20Matthew%20Fadayo%20PhD%20Thesis.pdf?sequence=1&isAllowed=y*

Fatoyinbo; O.V. (2018). Internal control and fraud prevention. Retrieved from: https://www.academia.edu/6207437/internal_control_and_fraud_prevention

Financial Fraud Action UK (FFA-UK 2011).Scams and computer viruses contribute to fraud increases – calls for national awareness campaign. *Press Release.*

Financial Fraud Action UK (FFA-UK, 2011). Fraud update: Payment cards, remote banking andCheque.

Finch, E.(2010).Strategies of adaptation and diversification : The impact of chip and PIN technology on the activities of fraudsters. *Security Journa, 56(7), 68-80.*

Fisher,B.S.,Daigle,L.E.,&Cullen,F.T.(2010).Unsafeintheivorytower:Thesexual victimization of college women. *Thousand Oaks, CA: Sage.*

Ganesan, R., &Vivekanandan, K. (2009). A secured hybrid architecture model for internetbanking (e-banking).*Journal of Internet Banking and Commerce, 14*(1), 1- 17.

Garson, G. D. (2008). Structural equations modelling, from statnotes: Topics in multivariate analysis. Retrieved from: htpp/:statnotes_strutural_equation_modelling/

Gates, T., & Jacob, K. (2009). Payments fraud: Perception versus reality. *Economic Perspectives, 33*(1), 7-15.

Geffner, M. (2014). How banks fight fraud in electronic banking. Retrieved from: www.banrate.com/how-banks-fight-fraud.

George, T. K., & Jacob, P. (2015).Fraud detection and mitigation in secure e-payment transaction.*InternationalJournalofScientific&EngineeringResearch,6*(2),1217- 1220.

Gertler, M., &Nobuhiro ,K.(2010).Financial intermediation and credit policy in business cycle analysis,in Friedman, Benjamin M., and Michael Woodford (Ed.), *Handbook of monetary economics* (pp. 547-599). Amsterdam, The Netherlands: Elsevier

Ghosh, A. K., Schwartzbard, A., & Schatz, M. (1999). Learning program behaviourprofiles for intrusion detection. Paper presented at the *Workshop on Intrusion Detection and Network Monitoring, 5(1),*1-13.

Giles, J. (2010). Scareware: The inside story. *New Scientist, 205*(27), 38-41.

Graham, J. R., Li, S., &Qiu, J. (2008).Corporate misreporting and bank loan contracting. *Journal of Financial Economics, 8 (9)*, 44-61.

Graycar, A., & Smith, R. (2002). Identifying and responding to electronic fraud risks. Paperesented at the *30th Australasian Registrars' Conference Canberra.*

Gunathilake, N., Padikaraarachchi, A., Koralagoda, S., Jayasundara, M., Paliyawadana, P.,Manawadu, C., &Rajapaksha, U. (2013).Enhancing the security of online banking systems via keystroke dynamics. Paper presented at the *Computer Science & Education (ICCSE), 2013, 8th International Conference,44(8),* 561-566.

Hamilton, D. I., Justin, M., &Odinioha, G. (2012,). Dimensions of fraud in Nigeria quoted firms.*American Journal of Social and Management Sciences, 3(3),* 112-120.

Hammud,I, Bizri, R.M.,& El baba, I. (2018). The Impact of E-Banking Service Quality on Customer Satisfaction: Evidence From the Lebanese Banking Sector. *SageJournals,8 (3),* 17-35.

Hoffman, D. G. (2002).*Managing operational risk: 20 firmwide best practice strategies.*London: John Wiley and Sons.

Hoehle, H., Scornavacca, E., & Huff. (2012). Three decades of research on consumeradoption and utilization of electronic banking channels: *A Literature Analysis. 54*(1), 122-132.

Holt, T. J., &Bossler, A. M. (2009).Examining the applicability of lifestyle-routine activities theory for cybercrime victimisation. *Deviant Behaviour, 30*(1), 25-54

Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the net? *Current Issues in Criminal Justice, 20*(3), 433-451.

Hutcheson, G. D., & Sofroniou, N. (1999). *The multivariate social scientist: Introductory statistics using generalized linear models*. New York: Sage.

Horn, R. (2010). *Designing a trading system.* Northway ZA: Alaziac Trading CC Nominee Old Tree Publishing.

Idogei S. O, Josiah, M &Onomuhara O. G (2017). Internal control as the basis for prevention, detection and eradication of frauds in banks in Nigeria. *International Journal of Economics, Commerce and Management, 5*(9), 61-88.

Idowu, A., &Adedokun, T. O. (2013). Evaluation of the effect of monitoring and control activities on fraud detection in selected Nigerian commercial banks. *Research Journal of Finance and Accounting, 4*(6), 37-54.

Iminza, N. W., Gikiri, W. l., &Kiragu, D. N.(2015). Operational governance and occupational Fraud Risk in commercial banks in Kenya. *European Journal of Business Management, 2*(1), 401-442.

Iwuagwu, O. (2000). Corruption: A threat to democracy and national development. *Journal of National Economic Group of Nigeria, 8*(1),12-16.

Jamieson, R., Stephens, G., & Winchester, D. (2007).An identity fraud model categorising perpetrators, channels, methods of attack, victims and organisational impacts. Paper presented at the *Pacific Asia Conference on Information Systems (PACIS),*2007 Proceedings.

Jansen, J., &Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands:Aqualitative analysis of factors leading tovictimization.*InternationalJournalofCyberCriminology,10*(1),79-91.

Josiah, M., Adediran, S. A., &Akpeti, O. E. (2012). Evaluation of roles of auditors in the fraud detection and investigation in Nigerian industries. *American Journal of Social and Management Sciences, 3*(2), 49-59.

Jassal, R. K., &Sehgal, R. K. (2013). Online banking security flaws: A study. *International Journal of Advanced Research in Computer Science and Software Engineering, 3(8)*,1016- 1021.

Jeffords, R., Marchant, M. L., &Bridendall, P. H. (1992). How useful are the tread way risk factors? *Internal Auditor, 5(8),* 60-62.

Johnson, M. (2008).*A new approach to internet banking.*(Unpublished PhD Thesis).University of Cambridge, Cambridge, UK. Retrieved from http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-731.pdf(731)

Karmen, A. (Ed.). (2010). *Crime victims: An introduction to victimology.* Belmont, CA: Cengage Wadsworth Learning.

Keivani, F. S., Jouzbarkand, M., Khodadadi, M., &Sourkouhi, Z. K. (2012). A generalview on the e-banking. Paper presented at the *International Proceedings of Economics Development & Research, 43*

Kennedy, L. W., &Forde., D. R. (1990). Routine activities and crime: An analysis of victimization in Canada. *Criminology, 28*(1), 137-151.

Kevin, W.,S., & Huang, W. (2011). The evolutional view of the types of identity thefts and online frauds in the era of the internet .*Internet Journal of Criminology,1(21*), 2045-6743

Kinkela, K., & Harris, P. (2014) .ACFE releases 2014 international study on internal fraud investigation, advocating internal audit. *Internal Auditing, 29*(5),10-14.

Kou, Y., Lu, C., &Sirwongwattana, S. (2004). Survey of fraud detection techniques.*In 2004 International Conference on Network, Sensing and Control, 17(6),* 749-754.

Kovach, S., & Ruggiero, W. V. (2011). Online banking fraud detection based onLocal and global behavior. Paper presented at *The Fifth International Conference on Digital Society,* Guadeloupe, France, 45(8), 166-171.

KPMG Forensic. (2006). *Guide to preventing workplace fraud. Taking action to reduce Businesscrime exposure.*

KPMG. (2000). E-commerce and cybercrime: New strategies for managing the risks of exploitation. *Forensic and Litigation Services, KPMG LLP, USA,* , 27 March.

Kranacher, M. J., Riley, R. A., & Wells, J. T. (2011).*Forensic accounting and fraudexamination*. London: John Wiley and Sons.

Kuponiyi, A. (2014). E-fraud:fighting the battle, winning the war in *e-Fraud: Fightingthe battle, Winning the war*: Nigeria Electronic Fraud Forum Annual Reports. 5(9),20-27.

Kumar, V.& Sriganga, B.K. (2014).A review on data mining techniques to detect insider fraud in banks, *International Journal of Advanced Research in Computer Science and Software Engineering, 4(12),* 370-380.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyber psychology, Behaviour, and Social Networking, 17*(8), 551-555.

Leung, A., Yan, Z., & Fong, S.(2004).On designing a flexible e-payment system with fraud detection capability. *56(4),*236-243.

Lister, L. M. (2007). A Practical Approach to Fraud Risk: *Internal Auditors*, *6(4)*,61-64.

Longo, E.,& Stapleton, J. (2002). PKI note: Smart cards. . *PKI Note Series,* PKI Forum.

Loonam, M., &O'Loughlin, D. (2008). An observation analysis of e-service quality in onlinebanking. *Journal of Financial Services Marketing,13*(2),164-178.

Mahdi, M.D.H., Rezaul, K.M., &Rahman, M.A. (2010). Credit fraud detection in the banking sector in UK: A focus on e-business. Paper presented at *theProc. of the 4th International Conference on Digital Society (10),* 232-237.

Malphrus, S. (2009), Perspectives on Retail Payments Fraud", *Economic Perspectives, 33(*1), 31-36.

Masocha, R., Chiliya, N., &Zindiye, S. (2011). E-banking adoption by customers in the ruralmilieus of South Africa: A case of Alice, Eastern Cape, South Africa. *African Journalof Business Management,5(5*),1857-1863.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviours utilizing routineactivity theory. *Deviant Behaviour, 31*(5), 381-410.

Meenatkshi, R., &Sivaranjani.K. (2016). Fraud detection in financial statement using data mining technique and performance analysis. *International Journal of Control Theory and Applications, 9(*27), 407-413.

Mhamane, S. S., & Lobo, L. M . (2012). Use of hidden markov model as internet banking fraud

detection. *International Journal of Computer Applications, 45*(21),7071-9556

Miller, J. (2013). Individual offending, routine activities, and activity settings: Revising the routine activity theory of general deviance. *Journal of Research in Crime and Delinquency, 50*(3), 390-416.

Mobarek, A. (2007) E-Banking Practices and Customer Satisfaction-A Case Study in Botswana, 20th Australasian Finance & Banking Conference.

Monrose, F., & Rubin, A. (2000). Keystroke dynamics as a biometric for authentication .*International Journal of Future Generation Computer Systems, 16*(4), 351-359.

Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T.,&Elovia, R. (2009).VerifiedbyvisaandMasterCardSecureCode: How not to Designauthentication.In R. Sion (Ed.), *Financial cryptography and data security,*60(5), 336-342.

Muscat, G., James, M., &Graycar, A. (2002).Older people and consumer fraud, *Trends and Issues in Crime and Criminal Justice, 2(20)*, 1-6.

Mukoro, O. D., Faboyede, O. S., &Eziamaka, C. B. (2014). The effectiveness of forensic accounting in strengthening internal control of business organization in Nigeria: A study of selected business organization in Nigeria. *Journal of Management Research, 6*(1), 40-69.

Mueller, K. (2015). How technology is shaping the fight against fraud? Assessed 25/3/2019 and available at www.inc.com/how_tech/

NDIC (2010).Perspectives on the Nigerian financial safety-net. An NDIC Book, Retrieved from http//:Downloads/Perspectives-On-the-Nigerian-Financial-Safety-net-NDIC-pdf

Nathan, M. (2019).Banking Fraud: Customers are Now the Most Targeted Fraud Vulnerability. Retrieved from: https://www.threatmetrix.com/digital-identity-blog/fraud- prevention/banking-fraud-customers-now-most-targeted-fraud-vulnerability/

Newman, G., & Clarke, R. V. (2003).*Superhighway robbery: Preventing e- commerce crime*. Portland, Willan Publishing.

Nigeria Interbank Settlement System(2014).Overview.Retrieved from:https://nibss-plc.com.ng/company-overview/

Njenga, N. M. &Osiemo (2013). Effect of fraud risk management on organization performance: A case of deposit-taking microfinance institutions in Kenya.*International Journal of Social Sciences and Entrepreneurship*, 1 (7), 490-507

Nkemdili, N. A., Bonaventure, U., & Kingsley, A. (2013). No light at the end of the tunnel: Corruption and insecurity in Nigeria.*Arabian Journal of Business and Management Review (Oman Chapter), 2(12*), 41-54.

Nor, K. M., Shanab, E. A. A., & Pearson, J. M. (2008). Internet banking acceptance in Malaysia

based on the theory of reasoned action. *JISTEM-Journal of Information Systems and Technology Management, 5(1*), 03-14.

Nwankwo, G. O. (2005). *Bank management principles and practices*, Lagos: Malthouse PressLtd

Nwankwo, O. (2013). Implications of fraud on commercial banks performance in Nigeria.*International Journal of Business and Management, 8(15),* 144-150.

Odediran,O.(2014).Holisticapproachtoelectronicchannelsfraudmanagement.*NigeriaElectronic Fraud Forum (NeFF) 2014 Annual Report.*

Odi, N. (2013). Implication of fraud on commercial banks performance in Nigeria, *International Journal of Business and Management, 8(15),* 144-150

Organization for Economic Cooperation and Development (1998). A borderless world: Realizingthe potential of global electronic commerce. *OECD Ministerial Conference on Electronic Commerce*, 7-9 October. Ottawa- Canada. Retrieved from: www.ottawaoecdconference.org/english/homepage.html

Ojo.(2008). Effect of frauds on banking operations in Nigeria.*International Journal of Investment and Finance, 1*(1), 103.

Oko, S., &Oruh, J. (2012). Enhanced ATM security system using biometrics. *International Journal of Computer Science Issues, 9(5),* 352.

Olorunsegun, S. (2010), The Impact of Electronic Banking in Nigeria Banking System (Critical Appraisal of Unity Bank Plc), A Master Degree Dissertation submitted to LadokeAkintolaUniversity of Technology, Ogbomoso, Oyo State, Nigeria.

Omar, A. B., Sultan, N., Zaman, K., Bibi, N., Wajid, A., & Khan, K. (2011). Customer perception towards online banking services: Empirical evidence from Pakistan. *Journal of Internet Banking and Commerce, 16*(2),1-24.

Omotayo, T. &Kulatunga, U. (2015). (2015). The research methodology for the development of a kaizen costing frame-work suitable for indigenous construction firms in Lagos, Nigeria. Paper presented at the ARCOM Doctoral Workshop Research Methodology, Grange Gorman Campus, Dublin Institute of Technology.

Orji, V.O. (2015). Knowledge management systems: Issues, challenges, and benefits. *Communications of the Association for Information Systems,1*(7), 223- 300.

Owolabi .S. A. (2010). Fraud and fraudulent practices in Nigerian banking industry.*African Research Review, 4(3),*240-256.

Pandey, M., (2010). A model for managing online fraud risk using transaction validation. *The Journal of Operational Risk, 5(1),*49-63.

Papazoglou, M. P.(2003). Web services and business transactions.*World Wide Web,6(1),*49-91.

Patil, R.A., &Renke, A.L. (2016). Keystroke dynamics for user authentication and

identification by using typing rhythm. *International Journal of Computer Applications 144*(9), 11-22.

Pedneault, S., Silverstone, H., Rudewicz, F., &Sheetz, M. (2012).*Forensic accounting and fraud investigation for non-experts. Washington DC:*John Wiley &Sons.

Perkins, E. D., & Annan, J. (2013). Factors affecting the adoption of online banking in Ghana: Implications for bank managers.*International Journal of Business and Social Research (IJBSR), 3*(6), 94-108.

Phua, C., Lee, V., Smith, K., &Gayler, R. (2012). A comprehensive survey of data mining-based fraud detection research. *ArXiv Preprint arXiv:1009.6119.*

Pratt, T. C., Holtfreter, K., &Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime andDelinquency,7*(3),267-296.

Polonsky, M. J., & Waller, D. S. (2005). *Research project: Designing and managing a business student guide*. California: Sage Publications Inc.

Pugesek, B., Tomer, A & Von Eye, A (2003). Structural equation modeling applications inecological and evolutionary Biology. Retrieved from: https://www.researchgate.net/publication/267657696_Structural_Equation_Modeling_Applications_in_Ecological_and_Evolutionary_Biology

Peled, S.G (2007).Video Surveillance in the Fight Against Bank Fraud. Retrieved from: https://www.cio.com/article/2438010/video-surveillance-in-the-fight-against-bank-fraud.html.

Rae, K., &Subramaniam, N. (2008).Quality of internal control procedures : Antecedents and moderating effect on organisational justice and employee fraud. *Managerial Auditing Journal, 23*(2),104-124.

Rajdeepa B.,&Nandhitha D. (2015). Fraud detection in banking sector using data mining. *International Journal of Science and Research (IJSR), 4*(7),1822-1825.

Ramamoorti, S,.Morrison, D.E., Koletar, J. W., & Pope, K. R. (2013).*A.B.C.'s of BehavioralForensics: Applying Psychology to Financial Fraud Prevention and Detection.* New York: John Wiley & Sons

Rampini, A. A., &Viswanathan, S. (2010). Collateral, risk management, and the distribution of debt capacity, *Journal of Finance*, *6(5),* 2293-2322.

Regha,O.(2015).Cybercrime:Ariskinformationcentretotherescue.*NigeriaElectronicFraud Forum (NeFF) 2015 Annual Report,* 4(9), 72-77.

Revett,K.,DeMagalhães,S.T.,&Santos,H.M.(2005).Passwordsecuredsitesstepping forward withkeystroke dynamics. in next generation web services practices. .Paper presented at the *NWeSP 2005. International Conference on IEEE,4(2),*11-28.

Revett, K. (2009). A bioinformatics-based approach to user authentication via keystroke dynamics. *International Journal of Control, Automation, and Systems, 7(1),* 7-15.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50(2),*216-238.

Reyns, B. W., & Henson, B. (2013).Security in a digital world: Understanding and Preventing Cybercrime Victimization. *Security Journal, 26(4),311-314.*

Reyns, B., Henson, B., & Fisher, B. S. (2011).Being pursued online: Applying cyber life style-routine activities theory to cyber stalking victimization. *Criminal Justice and Behaviour, 38(11),* 1149-1169.

Rizzardi, R. (2008). Financial management-payment card fraud can happen to you. *Optometry & Vision Development*, *39(2),* 64-65

Rossi, B.(2016).Top8 ways to fight mobile banking fraud. Retrieved from: https://www.information-age.com/top-8-ways-fight-mobile-banking-fraud-123460769/.

Roberds, W. (1998).The impact of fraud on new methods of retail payment.*Economic Review-Federal Reserve Bank of Atlanta, 83*(1), 42-52.

Sumner, D (2016). Six ways banks are fighting fraud with video based business intelligence. Retrieved from: https://securitytoday.com/articles/2016/03/16/six-ways-banks-are-fighting-fraud-with-video-based-business-intelligence.aspx

Saleh, Z. I. (2011). Improving security of online banking using RFID.*Academy of Banking Studies Journal, 10*(2), 1-16

Saunders, M., Lewis, P., & Thornhill, A. (2015). *Research methods for business students* (Seventh ed.). England: Pearson Education Limited.

Sarma, G., & Singh, P. K. (2010). Internet banking: Risk analysis and applicability of biometrictechnology for authentication. *International Journal of Pure and Applied Sciences and Technology, 1(2),* 67-78.

Schneier, B. (2011). *Secrets and lies: Digital security in a networked world.* New Jersey*:*John Wiley &Sons.

Shah, M. H.,Braganza, A., &Morabito, V. (2007). A survey of critical success factors in e-banking: An organisational perspective. *European Journal of Information Systems, 16*(4), 511-524.

Shanmugapriya, D., &Padmavathi, G. (2009). A survey of biometric keystroke dynamics: Approaches, security and challenges.*International Journal of Computer Science andInformation Security, 5*(1), 115-119.

Shannak, R. O. (2013). Key issues in E-banking strengths and weaknesses. *The Case of Two Jordanian Banks, European Scientific Journal, 9*(7), 239-263.

Silverstone,H.,&Sheetz,M.(2007).*Forensicaccountingandfraudinvestigation for nonexperts*(2nd ed.). New Jersey, USA: John Wiley & Sons, Inc.

Singh, P., & Singh, M. (2015).Fraud detection by monitoring customer behaviour and activities.*International Journal of Computer Applications, 111*(11), 23-32.

Shongotola, I.O. (1994). Fraud detection and control.*Nigeria Banker*, 16-19.

Soltani, B. (2013). The anatomy of corporate fraud: A comparative analysis of high profile American and European corporate scandals.*Journal of Business Ethics, 120*(2), 251-274.

Srivastava,A.,Kundu,A.,Sural,S.,&Majumdar,A.(2008).Creditcardfrauddetection using hidden Mmarkov model .*IEEE Transactions on Dependable and Secure Computing, 5*(1),37-48.

Sruthi T.V., &Prasanna, E. (2016). Fraud detection in banking institutions.*International Journal ofEngineering and Technology, 8*(2), 1127-1130.

Subramanian, R. (Ed.). (2014). *Bank fraud: Using technology to combat losses*. North Carolina, USA.: SAS institute Inc.

Sullivan,R.J.(2014).Controllingsecurityriskandfraudinpaymentsystems.*Economic Review-Federal Reserve Bank of Kansas City, 8(6), 15*-36.

Symantec Security Response.(2005). Phishing in the middle of the stream - Today's threats to online banking. Paper presented at the *The AVAR 2005 Conference,* Symantec Security Response, Dublin. 6(2), 1-28.

Tan,T.M.,&Rasiah,D.(2011).Areviewofonlinetrustbrandingstrategiesoffinancial services industries in Malaysia and Australia*., Advances in Management & Applied Economics, International Scientific Press, 1*(1),125-150.

Taylor, J. (2011). *Forensic accounting*.England: Pearson education.

Tewksbury, R., &Mustaine, E. E. (2001). Lifestyle factors associated with the sexual assault of men: A routine activity theory analysis. *The Journal of Men's Studies, 9*(2),153-182.

Tillyer, N.,&Eck, E. (2009). *Crime prevention: criminal justice series*. Pennsylvania State University:Willan Publishing.

Tongce, M. D. C. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research and Applications,5(9),* 147-158.

Tseloni, A., Wittebrood, K., Farrell, E., &Pease, R. (2004). Burglary victimization in England and Wales, theunited states and the Netherlands: A cross national comparative test of routine activities and lifestyle theories. *British Journal of Criminology, 4*(1), 66-91.

Uchenna, C., &Agbo J. C. (2013).Impact of fraud and fraudulent practices on performance of banks in Nigeria.*British Journal of Arts and Social Science, 15*(1), 55-95.

Udoayang,J.O.,&James,F.U.(2004).*Auditingandinvestigation.*Calabar:University ofCalabar Press.

Usman, A. K., & Shah, M. H., (2013). Critical success factors for preventing e-banking fraud. *Journal of Internet Banking and Commerce, 18*(2), 1-15.

Vandommele, T. (2010).Biometric authentication today.*Seminaron Network Security,* 1(10), 52- 90

Velicer, W. F., Eaton, C. A., & Fava, J. L. (2000). Construct explication through factor or component analysis: A review and evaluation of alternative procedures for determining the number of factors or components.Problems and solutions in human assessment (pp. 41-71) Springer

Wada, F., &Odulaja, G. (2012).Assessing cybercrime and its impact on e-banking in Nigeria using social theories. *African Journal of Computing & ICT, 5*(1), 69-82.

Wang, S. K., & Huang, W. (2011). The evolutional view of the types of identity thefts and online frauds in the era of the interne. *Internet Journal of Criminology,1(11),* 14-22.

Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J. (2012).Effective detection of sophisticated onlinebanking fraud on extremely imbalanced data.*World Wide Web (Internet and Web Information Systems),* doi:10.1007/s11280-012-0178

Wells, J.T.(2005).New approaches to fraud deterrence.*The Chartered Accountant,14(5),*3-14.

Wells, J. T. (2014). New Approaches to Fraud Deterrence.*The Chartered Accountant*.*The Institute of Chartered Accountants of India*, 23(9), 1453-1455.

Wilcox, P., Madensen, T. D., &Tillyer, M. S. (2007). Guardianship in context: Implications For burglary victimisation risk and prevention', *Criminology,* (44),771-803.

Wilhelm, W. K. (2004). The fraud management lifecycle theory: A holistic approach to fraud management. *Journal of Economic Crime Management, 2*(2), 1-38.

Williams, M. L. (2015). Guardians upon high: An application of routine activities theory to onlineidentity theft in Europe at the country and individual level. *British Journal of Criminology, 56*(1), 21-48.

Williams, M. L., (2016). Perceptions of the e-Crime controllers: Modelling the influence of cooperation and data source factors Security. Article*,* doi:10.1057/sj.2012.47.

Wilsem, J.A. (2011). "Bought it, but never got it'' Assessing risk factors for online consumer fraud victimization. *European Sociological Review*.*Oxford: Oxford Univ. Press,*

Wilsem , J. A. (2013). Bought it, but never got it: Assessing risk factors for online consumer fraud victimization. *European Sociologic Review, 29*(2),168-178.

Wisdom, K. (2012).*The impact of electronic banking on service delivery to customers of*

Ghanacommercial bank limited.(Ph.D. Thesis,).

Wolfe, D. T., &Hermanson, D. R. (2004). The fraud diamond: Considering the four elements offraud.*The CPA Journal, 74*(12), 38-42.

Yamane, T. (1967). *Statistics: An introductory analysis*. New York: Harper and Row.

Yan, A. W., Md-Nor, K., Abu-Shanab, E., &Sutanonpaiboon, J.(2009). Factors that affect mobiletelephone users to use mobile payment solution. *International Journal of Economics andManagement, 3*(1),37-49.

Yar, M. (2005).The novelty of 'Cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427.

Zimucha, T., Zanamwe, N., Chimwayi, K., Chakwizira, E., Mapungwana, P., &Maduku,T. (2012). An evaluation of the effectiveness of E-banking security strategies in Zimbabwe:A case study of Zimbabwean commercial banks. *Journal of Internet Banking and Commerce, 17*(3), 1-16.

E-BANKING SYSTEM AND FRAUD PREVENTION IN NIGERIAN MONEY DEPOSIT BANKS

SECTION A: Demographic Data

Instruction: Please, mark the appropriate box for the option that best describes you.

1. Gender: Male ☐ Female ☐

2. Age (years):Below 20 ☐ 20-30 ☐ 30-40 ☐ 41-50 ☐ Above 51 ☐

3. Marital status: Single ☐ Married ☐ Divorced ☐ Separated ☐

4. Highest Educational Qualification: OND ☐ BSc/HND ☐ MSc/MBA ☐

Others (Specify).....

5. Type of Account:Savings ☐ Current ☐ Fixed Deposit ☐ Others.....

6. Societal Class: High ☐ Middle ☐ Low ☐

SECTION B: LIKERT STRUCTURED QUESTIONS

Please, tick your level of agreement with the statement below, Strongly Agreed (5), Agreed (4), Undecided (3), Disagreed (2), Strongly Disagreed (1)

PART ONE: E-Banking system in Nigeria Deposit Money Bank							
S/N		5	4	3	2	1	
1	The evolution of E-banking system has brought a paradigm shift in banking transaction.						
2	Incidences of Identity theft is prominent toNigeria e- banking channels.						
3	Online hacking is of high concern to e-banking channels in Nigeria						
4	ATMs Fraud like skimming, shoulder surfing, card theft, pin hijacking is of high concern to Nigeria deposit money banks						
5	Collusion between banks staff and online fraudsters is a common Occurrence in Nigeria deposit money banks.						
6	Anonymous messages, emails, telex and calls requesting customers information are prevalent to Nigeria e-banking system.						
7.	Low customer/staff internet banking awareness rises online						

fraud incidence

Technological mechanism as a Preventive Tool						
S/N		5	4	3	2	1
8	If there exist sophisticated forensic technological tools I believe e-banking fraud would be prevented					
9	One-time password (OPT, MasterCard Secured code and Verified by Visa (VBV) are crucial for effective online banking in Nigeria					
10	I believe the usage of dedicated phone lines, emails, and equipped customer service centrecan limit the incidence of e-banking fraud					
11	If automated data analysis and transaction monitoring software are put in place e-banking fraud will abate					
12	Monitoring threats to internet banking activities such as phishing, pharming, hacking, site cloning, etc is a necessity in tackling online banking fraud in Nigeria					
13	Periodic technological/system upgrade does not allows fraudsters taking advantage of loopholes in e-banking channels					
14	The use of automated address system (AVS), Bank Verification Number (BVN) and Google mapping are idea for preventing fraud					
S/N	**Customer Whistle Blowing as a preventive Measure**					
15	If dedicated channels for customer complains (hotlines) are put in place, I believe fraud activities in e-banking will reduce					
16	Viable customer service desk, employment of well trained customer service officers enhances anti-fraud in online banking					
17	Following up/resolving customers complains will hinder fraudsters from taking over online banking platforms.					
18	Viable whistle blowing policies in Nigeria deposit money banks will abate e-banking fraud					
19	Entertaining whistle blowing/anonymous information is a measure for fighting e-banking fraud					
20	Keeping identity of whistle blowers will facilitate whistle blowing effectiveness in Nigerian banks					
21	Rewarding whistle blowers will encourage whistle blowing activities					
S/N	**Surveillance Mechanism for Fraud Preventive Measure**					
22	Intelligent gathering tactics is a measure to fight fraud in Nigeria online banking channels					
23	Use of token, Pin codes, Passcodes and memorable words enhances an effective fraud-free banking					

24 CCTV and web cameras at transaction points is a must for tackling activities of fraudsters

25 Deployment of trackers, customers footage will prevent fraud from taking place

26 If deployment of securities officer around e-banking channels is taking seriously, will not easily occur.

27	Monitoring of ATMS and outdoors e-banking channels will not permit fraudsters from taking advantage of banking services					
28	Employment of misery shoppers will not allow e-banking robbers in taking advantage of bank employee weakness					
S/N	**Staff/Customer Awareness/Education as a Fraud Preventive Measure (Control Variable)**					
29	Customer enlightenment campaign and publicity will guard against fraud in Nigerian deposit money banks					
30	Fraud awareness training for staff and anti-fraud tips will easily expose fraudulent attempts/red flags					
31	Display of suggestion boxes in banking hall can serve as a means of preventing fraud					
32	Subscribing business news letter, magazines and television enlightment channels will educate staff/customers for falling victim.					
33	Showcasing product/service information on screen display in banking Halls, bank websites and advertorials is an antifraud agents					
34	Usage of short code e.g USSDs and help yourself platforms are transactions monitoring mechanisms					
35	Dedicated web pages for customer enquiries, product enlightenments and education has the capacity to reduce fraud					

APPENDIXES

Sex

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	39	46.4	47.0	47.0
	1	44	52.4	53.0	100.0
	Total	83	98.8	100.0	
Missing	System	1	1.2		
Total		84	100.0		

Source: Eviews,8.0

Education

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	12	14.3	14.5	14.5
	2	43	51.2	51.8	66.3
	3	9	10.7	10.8	77.1
	4	19	22.6	22.9	100.0
	Total	83	98.8	100.0	
Missing	System	1	1.2		
Total		84	100.0		

Source: Eviews,8.0

Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	70	83.3	84.3	84.3
	2	6	7.1	7.2	91.6
	3	6	7.1	7.2	98.8
	4	1	1.2	1.2	100.0
	Total	83	98.8	100.0	
Missing	System	1	1.2		
Total		84	100.0		

Source: Eviews,8.0

Marital status

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	62	73.8	74.7	74.7
	2	7	8.3	8.4	83.1
	3	13	15.5	15.7	98.8
	4	1	1.2	1.2	100.0
	Total	83	98.8	100.0	
Missing	System	1	1.2		
Total		84	100.0		

Source: Eviews,8.0

Societal Class

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	18	21.4	21.7	21.7
	2	32	38.1	38.6	60.2
	3	33	39.3	39.8	100.0
	Total	83	98.8	100.0	
Missing	System	1	1.2		
Total		84	100.0		

Source: Eviews,8.0

Type of Account

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	20	23.8	24.1	24.1
	2	23	27.4	27.7	51.8
	3	19	22.6	22.9	74.7
	4	21	25.0	25.3	100.0
	Total	83	98.8	100.0	
Missing	System	1	1.2		
Total		84	100.0		

Source: Eviews,8.0

Reliability Statistics

Cronbach's Alpha	N of Items
.836	35

Source: Eviews,8.0

Dependent Variable: FP
Method: Least Squares
Date: 11/15/19 Time: 11:04
Sample (adjusted): 2 83
Included observations: 82 after adjustments
Convergence achieved after 5 iterations
White heteroskedasticity-consistent standard errors & covariance

Variable	Coefficient	Std. Error	t-Statistic	Prob.
CWB	0.428506	0.123847	3.459970	0.0009
SUVMEC	0.444949	0.121308	3.667917	0.0005
TECMEC	-0.100217	0.156635	-0.639812	0.5242
SCAE	-0.219582	0.081012	-2.710503	0.0083
C	1.400116	0.246097	5.689280	0.0000
AR(1)	0.000352	0.119217	0.002952	0.9977

R-squared	0.468306	Mean dependent var	2.753659
Adjusted R-squared	0.433326	S.D. dependent var	0.773830
S.E. of regression	0.582522	Akaike info criterion	1.827456
Sum squared resid	25.78922	Schwarz criterion	2.003557
Log likelihood	-68.92569	Hannan-Quinn criter.	1.898158
F-statistic	13.38789	Durbin-Watson stat	1.984692
Prob(F-statistic)	0.000000	Wald F-statistic	33.94307
Prob(Wald F-statistic)	0.000000		

Inverted AR Roots	.00

Source: Eviews,8.0

Heteroskedasticity Test: Breusch-Pagan-Godfrey

F-statistic	0.246926	Prob. F(4,77)	0.9107
Obs*R-squared	1.038518	Prob. Chi-Square(4)	0.9039
Scaled explained SS	0.895407	Prob. Chi-Square(4)	0.9252

Source: Eviews,8.0

Test for Misspecification

Ramsey RESET Test
Equation: UNTITLED
Specification: E_BANK COMP SUVMEC TECMEC SCAE C AR(1)
Omitted Variables: Squares of fitted values

	Value	Df	Probability
t-statistic	1.159170	75	0.2501
F-statistic	1.343676	(1, 75)	0.2501
Likelihood ratio	1.456081	1	0.2276

Source: Eviews,8.0

Data for the Study

FP	CWB	SUVMEC	TECMEC	SCAE
2.6	2.4	2.8	2	3.4
2	1.6	1.8	2	3.4
2	1.6	2	2.2	3
3.2	1.4	2.6	2.2	2.6
2.4	1.2	2.4	1.6	2.4
2.8	1.6	2	1.6	2
3	2.4	1.6	3	1.6
2.8	2.2	3.2	2.6	3.2
2.4	1.4	3.2	2.2	3.2
1.6	1.2	1.6	2.4	1.6
2.6	1.8	2.6	2	2.6
3.8	3.6	3.8	2.8	3.8
3	3.6	3.6	3.6	3.6
2.6	4.4	4.2	4	4.2
4.2	4.2	4	4	4
2.6	2.6	2.8	2.6	2.8
1.6	1.2	1.6	2.4	1.6
4.2	4.2	4.2	4.6	4.2
4.2	4.2	4	3	4
3.4	3.6	3.6	3.6	3.6
2.8	3.6	4.2	3.8	4.2
3	3.6	4.4	4.2	4.4
2.4	3.4	4.4	2.8	4.4
3.6	3.4	3.2	3.8	3.2
3.8	3.6	4.2	3.6	4.2
4.2	3.6	3.6	2.8	3.6
2.6	3.4	3	2.4	3
3	2	2.6	2.6	2.6
1	2	2	3.4	2
3.2	1.4	2.4	3	2.4
4	3.2	3.6	3.4	3.6
2.2	2.2	3.2	2.4	3.2
2.4	2	1.6	2.6	1.6
2	2	2	1.8	2
2.8	1.8	3.2	2.2	3.2
4	2	2	2	2
4	3	2.4	1.6	2.4
2	2	0	2	0
2.6	3	2.4	3.2	2.4
2	1.8	2.4	2.2	2.4

1.8	1.8	2.4	2.2	2.4
1.2	1.6	2.2	2.2	2.2
2.8	2.2	2	1.6	2
3.8	4.4	4.2	3.8	4.2
2.4	2.6	2.2	3	2.2
2.4	1.8	1.8	2.2	1.8
3.2	2.6	2.2	1.8	2.2
2.4	1.4	2.8	2.4	2.8
3.4	2.8	1.6	1.6	1.6
4	4.2	4.4	3.4	4.4
2.4	2.6	2.8	2	2.8
2.6	2.4	2.6	2.4	2.6
2.4	2.6	2.6	2.6	2.6
1.6	0	0	0	0
0.4	0	0	0	0
3.2	2.4	3	1.8	3
1.8	1.2	2.4	2	2.4
3	2.4	1.8	2.4	1.8
2.6	2.2	3	3.4	3
2.6	2.2	3.2	2.6	3.2
2.6	2.6	2.8	2.4	2.8
2.4	2.6	2.8	2.4	2.8
3.2	2.2	2.2	2.2	2.2
3.8	3.4	4.4	3.2	4.4
2.6	1.8	2.8	3	2.8
3.2	1.4	2	2.4	2
2.6	1.8	2.8	3	2.8
2.8	2	3	2.8	3
3.2	2	1.6	2.4	1.6
1.6	1.8	1.8	1.8	1.8
3.2	2.8	2.8	3	2.8
2.4	1.2	2.4	1.6	2.4
3	2.2	2.4	2.4	2.4
2	1.2	2.6	2	2.6
4	1.6	4.4	2.4	4.4
2.8	2	1.8	3.2	1.8
2.2	2.4	3	2	3
2.6	3	3.4	3.2	3.4
2.6	2.4	2	1.8	2
2.6	1.8	2.8	2.4	2.8
2.2	1.4	2.6	1.8	2.6
3	3	3	3	3
3.2	1.8	3	2.6	3