Sociological Analysis of Internet Banking Fraud in Nigeria: Patterns and Effects

Okeh, Peter Igboke[1], Onuoha, Ogobuchi Onuoha[2], Ebeke, Walter Ibiam[3], Echee Solomon Amechi[4]

[1,3]Department of Criminology and Security Studies, Alex Ekwueme Federal University, Ndufu-Alike, Abakaliki,

[2]Department of Sociology, Ebonyi State University, Abakaliki

[4]Department of Psychology, Ebonyi State University, Abakaliki

DOI: https://dx.doi.org/10.47772/IJRISS.2025.90400196

Received: 15 March 2025; Revised: 31 March 2025; Accepted: 03 April 2025; Published: 06 May 2025

ABSTRACT

The phenomenal growth in the number of those who subscribe to internet banking around the world, and particularly in Nigeria, has led to an increase the number of potential Nigerians vulnerable to internet banking fraud victimization. The main thrust of the paper is to explore sociologically the causes and effects of internet banking fraud on the residents in Nigeria who are using banking services. The study being basically a review one and theoretical in nature, relied primarily on secondary data involving the use of internet to access related/relevant literature. Strain and Fraud diamond theories formed the theoretical orientation of the study. From the review, the study found that morbid desire to get rich quick and insecurity of job are the major causes of internet banking fraud. Credit card/debit card fraud and identity thefts are the two patterns of internet banking fraud. While Lack of trust among the banking public was the major effect. However, the study recommends among others, for government agencies, law enforcement agencies, intelligence agencies and security agencies to fight curb internet banking fraud. There is need for them to understand both the technology and individuals who engage in internet banking fraud.

Keywords: Internet, Banking Fraud, Patterns, Effects

INTRODUCTION

The internet is the amalgamation of network of computers which enables organizations as well as individuals to engage in communications electronically, assists in the conduct of businesses, sharing of and accessing already stored information. The World Wide Web (www) and the internet are the most widely used information channels ever (Laukkanen, 2007). However, advancement recorded so far in technologies, especially those related to communications and information are attracting attention in business transactions; the banking industry is however not an exception (Lichtenstein & Williamson, 2006).

Conversely, the popularity of internet banking has led to an increase in frauds. It soared as banks push us towards a digital future (Foley & Jayawardhena, 2000). Internet banking frauds occurs when someone uses another person's details to access his/her account in internet banking, and illegally transfers funds to a different financial institution. Internet banking frauds are difficult to analyse and detect because the fraudulent behavior is dynamic, spread across different customer profiles, and dispersed in large and highly imbalanced datasets (e.g., web logs, transaction logs, spending profiles) (Miro, 2014). Internet banking frauds are swift, clean, non-violent, sophisticated and sometimes untraceable (Cao et al, 2013). It is distinguished from bank robbery by the fact that the perpetrator keeps the crime secret, in the hope that no one notices until he has gotten away (Content team, 2015).

Internet banking has created new opportunities for frauds, as transactions are faster, do not require any human intervention, and are often “anonymous” (Oracle, 2012). Due to the pivotal roles of banks in the growth and

economic development of any nation, it has become very necessary to protect these institutions from the antics of fraudsters (Ikechi & Okay, 2013).

In 2010, data released by Financial Fraud Action, has indicated that there has been a 14 percent increase in internet banking frauds, $53million in 2008 to $60million 2009, which summed up to overall total of increase of $48 million since the first-time internet banking fraud case was reported in the year. This increase is due to a rise in usage of more sophisticated tool by the perpetrators who are mostly bank employees (FFA UK, 2010).

The South African Banking Risk Information Centre (SABRIC, 2019) reported that, in 2017, a total of 13,438 internet fraud cases involving mobile and banking apps as well as online reportedly costed the banking industry a gross sum of more than R250,000,000. The rate of internet crime and economic crime is reportedly increasing in the South African financial institutions (Cassim, 2016; PWC, 2016; Van, 2017). According to Mbelli and Dwolatzky (2016); Van, (2017) and PWC (2020), internet fraud is still a threat to the South African banking sector, despite the efforts of the sector to mitigate its occurrences They indicated that the rate of cybercrime is increasing globally with dire consequences on the customer's satisfaction, reputation and economic growth of financial institutions. Other losses include the indirect loss via loss of trust in the digital infrastructure, direct loss through fraud perpetration, as well as customer and stakeholder losses (Kraemer Mbula, Tang, & Rush, 2013).

Besides, the difficulty of checking identity and legitimacy online, the ease with which fraudsters or hackers can divert browsers to dishonest sites and steal credit card details, the international dimensions of the web and the ease with which users can hide their location, all contribute to making internet banking frauds the fastest growing area of fraud. Estimates are that just twenty percent of frauds are exposed and made public. The remaining frauds are either undetected or discovered and not made public because of reputation risk (Ballantine & Bartlet, 2002).

Furthermore, data released by the Central Bank of Nigeria (CBN, 2015) revealed that the banking sector lost over N3.04 billion in 2014 to internet banking frauds. The report also stated that although the total amount involved in these cases dropped to N9 billion at the end of December 2014 from N16.82 billion recorded in the first half of 2014, the actual losses from the incidents increased to N3.04 billion at the end of December 2014, from N1.72 billion in the first half of 2014. The Financial Stability Report (FSR) covered activities in the financial sector between June and December, 2014. The report observed that some of the reported cases of internet banking frauds were perpetrated by employees of banks and in jurisdictions with less secure payment platforms. The report further noted that 2014 was quite alarming in terms of internet banking frauds, as it recorded very high volume of fraudulent transactions. Unreported cases, according to the report, were far higher than the reported cases of fraud perpetrated in the system. Despite efforts to ensure that banks adopt global best practices such as the latest version of the Payment Card Industry Data Security Standard (PCIDSS) certification to mitigate the cyber-threat to their systems, the banking watchdog revealed that total losses by the nation's lenders due to internet banking frauds and related cases had gotten to about N203 billion in the last 14 years. The report also expressed concern that fraudsters (employees involved in the act) are so ingenious these days that they usually find ways of getting around security measures put in place to checkmate their activities. It stated that as many as 20 or 30 employees in collaboration with others are often involved in most internet banking frauds (Adepoju, 2014).

There is no doubt that this is a major problem that must be seriously tackled. Though not peculiar to Nigeria as other nations face similar challenge, internet banking frauds is capable of crippling the banking sector. In 2016 alone, several banks in Nigeria have reported less than anticipated profit returns. This may not be unconnected with millions that these fraudsters (employees) may have succeeded is siphoning out of the system (Oladeinde, 2017). Fraudsters thrive on the vulnerability of a bank's security system. Once the system is weak, it becomes susceptible to steal funds. There is no doubt that much has been done by banks in this securing their system. However, a lot more need to be done since internet banking fraud cases continue to be on the rise (PmnewsNigeria, 2015).

Thus, in nutshell, "inadequate measures to prevent internet banking fraud is the primary reason for widespread frauds. Technology (internet) is like a double-edged sword, which can be used to perpetuate, detect and prevent frauds" (Bhasin, 2013:67). It is against the foregoing problems that this study seeks to answers to the following

questions:

1. What are the causes of internet banking frauds in Nigeria?
2. What are the patterns of internet banking frauds in Nigeria?
3. What are the effects of internet banking frauds in Nigeria?

LITERATURE REVIEW

Related literatures and theories were reviewed in line with the study.

Causes of Internet Banking Frauds

Idolor (2010), sets out to find the common types of bank fraud that are frequently carried out in the banking system, the underlying causes, level of staff involvement, consequences and possible means of ameliorating the problem in Nigeria. Studying a sample of 100 respondents taken in Benin City, capital of Edo State, Nigeria by means of field survey questionnaire and testing the responses for significance using the "t-test", he found that respondents did not view unofficial borrowing and foreign exchange malpractice as forms of bank fraud since they were common and an industry wide practice. It also revealed that there was an equal level of staff involvement in initiating and executing fraud, with the concealment of fraud coming last in their agenda. Also, among the factors hypothesized to encourage bank fraud; the major individual based factors were greed, infidelity and poverty, while organizational factors were inadequate staffing, poor internal controls, inadequate training and poor working conditions. Respondents also viewed greed, lack of personal ethics and weak corporate governance as managerial factors that help propagate frauds in banks.

Adeyemo (2012) examined frauds in Nigerian banks: nature, deep-seated causes, aftermaths and probable remedies for banks in Nigeria. He used descriptive research method. The research study leaned heavily on the Nigerian Deposit Insurance Corporation NDIC) annual reports for data relating to total amount involved in frauds and forgeries. Ten banks with the highest fraud cases and categories of bank staff involved in frauds and forgeries from 2000-2009 were examined. He concluded that the battle for the preclusion, uncovering and retribution of fraud offenders must be fought on two extensive fronts: First is to reduce the temptation to commit fraud and second to increase the chances of detection. While a positive work environment will help to achieve the former, the latter can be achieved by sound internal control system.

Akindele (2011) set out to identify the internal bank fraud in Nigeria, its impact and identify means of controlling it. The study used the survey research method and his major findings revealed that lack of adequate training, communication gap and poor leadership skills were the greatest causes of fraud in the Nigerian banking Industry. The author therefore recommended that adequate internal control systems should be put in place and that workers satisfaction and comfort should be taken care of.

Ewa and Odoayang (2012) conducted a study on the impact of internal control design on banks' ability to investigate staff fraud, and life style and fraud detection in Nigeria. The study used descriptive research and findings of their study indicated that, internal control design influences staff attitude towards fraud, that a strong internal control mechanism is a deterrent to staff fraud while a weak internal control mechanism exposes the system to fraud and creates opportunity for staff to commit fraud. That most Nigerian banks do not pay serious attention to the life style of their staff members and that most staff members are of the view that effective and efficient internal control design could detect employee fraud schemes in the banking sector.

According to Adebisi (2009), the causes of internet banking frauds can be categorized into two: institutional factors and environmental/societal factors. Institutional factors, according to Nwaze (2008), can be traced to internal environment of the organization. A major institutional cause of fraud is poor management which comes in the form of inadequate supervision. Staff that has access to internet with fraudulent tendencies that is not adequately supervised would get the impression that the environment is safe for the perpetration of frauds. Poor management also manifest in ineffective policies and procedures, which a fraudulent minded operator in the system will capitalize on. Overstretching is another reflection of poor management. This can aid perpetration of fraud to a large extent. A staff that is overstretched is not likely to perform at optimum level of efficiency.

External/Environmental factors: Environmental factors are those that can be traced to the banks immediate and remote environment. Asukwo (2009) noted that the present society is morally bankrupt, little or no premium is put on things like honesty, integrity and good character. The society does not question the source of wealth. According to him, the immediate and remote causes of internet banking frauds in general include the following: greed, inadequate staffing, poor internal control, inadequate training, and poor book keeping and genetic traits. Other factors may include: frustration, slow and tortuous legal process, lack of effective deterrent or punishment and at times redundancy on the part of the individual bank to report frauds due to the perceived negative publicity it could create for the image of the institution (Asukwo, 2009).

Additionally, Idowu (2009), identified some other causes internet banking frauds which include the following:

(i) Poor Internal Control: Inadequate internal control and checks usually creates a loophole for fraudulent staff, and non-customers to perpetrate frauds. Therefore to reduce or eliminate frauds, there is a need to always have effective audits, security systems and ever observant surveillance staff at all times during and after bank official operating hours.

(ii) Greed: Greed refers to an inner drive by which individuals acquire financial gains far beyond their income and immediate or long-term needs. It is usually driven by a morbid desire to get rich quick in order to live a life of opulence and extravagant splendor. Greed has in many cases been regarded as the single most important cause of fraud in the banking sector.

(iii) Inadequate Staffing: A poorly staffed bank will usually have a problem of work planning and assignment of duties. The bank that is flooded with incompetent and inexperienced staff will of a necessity have to struggle with the problem of training and supervision of its officers. This situation can very easily be capitalized upon by the teeming fraudsters that the bank has to contend with in its day to day business.

(iv) Inadequate Training and Re-Training: Lack of adequate training and retraining of human resources both on the practical and theoretical aspects of banking activities and operations more often than not leads to poor performance. Such inefficient performance creates a loophole which can very easily be exploited by staffs.

Other subsequent factors suggested by Idolor (2010), also includes:

- .Inadequate compensation, salaries and fringe benefits which are accruable to bank staff.
- Refusal to comply with laid-down procedures without any penalty or sanction.
- Conspiracy between interacting agents charged with the responsibility of protecting the assets and other interest of the bank.
- Poor working conditions.
- Poverty and infidelity of employees.

The Patterns of Internet Banking Frauds

Some of the ways by which fraudsters defraud unsuspecting members of public and banks via the internet includes: Credit card/debit card fraud and identity theft are two patterns of internet banking frauds which are normally used interchangeably. It involves impersonation and theft of identity (name, social insurance number (SIN), credit card number or other identifying information) to carry out fraudulent activities. It is the unlawful use of a credit/debit card to falsely obtain money or belongings without the awareness of the credit/debit card owner (Dube, Mashanyanye & Njanike, 2009).

Theft of someone's identity can be done through different ways. According to Barker, D'Amato and Sheridon (2008), skimming involves stealing information off a credit card during a legitimate transaction. This type of scheme usually occurs in a business where the patron's credit card is taken out of sight while the transaction is being processed. The fraudster will swipe the card through an electronic device known as a "wedge" or skimming device, which records all information contained on the magnetic strip (ACFE, 2007) cited by Barker et al. (2008). To obtain credit card details, offenders may employ sophisticated method such as hacking into merchants' databases or simply "engineering" the victims into giving their credit card details (Prabovo, 2011). However, in

an attempt to maximise the benefits from technology utilization most people end up being victims of technology. Some fraudsters design web pages to look like legitimate sites where victims enter personal information such as usernames, passwords and credit card details. Often emails are sent to recipients asking disclosure and/or verification of sensitive information, and upon disclosure of such information the offenders make online transfers (Barker et al., 2008). Smishing and vishing are forms of phishing which are more sophisticated and uses phone text messages and phone calls to bait victims (KPMG, 2012; Tendelkur, 2013). This kind of fraud can also be used to target corporate and other merchants. E-commerce merchant sites have been a target as they normally contain valuable loyalty points or stored payment card information that can be used for fraudulent purchases and also a kind of mass-marketing fraud (Dowling & McGuire, 2013).

Traditionally, fraud perpetrators in bank institutions used "pen and paper" to commit internal fraud. However, upon computerisation of the transactions the same perpetrators shifted to internet or online frauds committing the same type of fraud (Shinder, 2002). In some cases, staff (fraudsters) run a programme known as the "salami technique" as an approach to steal money in small increments. The programme makes micro-changes over an extended period, so that the changes are not easily noticeable. An example of this type of fraud is a programme that deducts a few dollars per month from the accounts of many clients (Tendelkur, 2013). In the recent global recession period money laundering and/or cyber laundering has been a common unethical practice. It is a form of fraud that involves the electronic transfer of funds to launder illegally obtained money. The competence to transfer limitless amounts of money without having to go through strict checks makes cyber money laundering an attractive proposition (Ikechi & Okay, 2013; Rehman & Siddique, 2011; Shinder, 2002). New technologies and internet offer money launderers new opportunities and present new challenges to law enforcement and difficulties in the investigations of internet-based-money laundering techniques (Gercke, 2011; SiongThye, 2002).

Effects of Internet Banking Frauds

Dimejesi (2004), examined that the effects of the epidemic called fraud had hit the banking industry in Nigeria, leading to the loss of confidence by the public in banking institutions. He pointed out that the incidence of fraud is universal and permeates the society as a whole. However, in his research study, survey method were used, He narrowed down his scope to the commercial and merchant banks in order to take a meaningful study. Research data used were extracted from two out of four types of banks that make up the banking industry in Nigeria. The four categories include-commercial banks, merchant banks, development banks and the central bank of Nigeria. This was considered necessary since the banks render different types of services and as a result, prone to different kinds of frauds. The study findings revealed that fraud has mainly accounted for the decline in the profits of banks.

Okoye and Gbegi, (2013), analyzed the impact of banking frauds and related financial crimes on the growth and development of Nigerian economy. Analyzing the secondary data generated using regression analysis. The research findings revealed that, fraud and related financial crime has significant effect on the Nigerian economy. The research recommended that auditors and accountants in financial institutions should be trained on how to carry out forensic investigation given the current trend and strengthen their internal control systems.

Eseoghene (2010) stipulates that "nowhere are frauds more serious and more pronounced than in the banking sector of the economy; they are one of the biggest single causes of bank failure and distress in the Nigerian banking system." His work sets out to find the common types of bank frauds that are frequently carried out in the banking system, the underlying causes, level of staff involvement, consequences and possible means of ameliorating the problem. Analyses of data collated through questionnaire were tested for significance using the "t-test". The analysis revealed that respondents did not view unofficial borrowing and foreign exchange malpractice as forms of bank fraud since they were common and an industry wide practice. It also revealed that there was an equal level of staff involvement in initiating and executing fraud, with the concealment of fraud coming last in their agenda. Among the factors hypothesized to encourage banking frauds; the major individual based factors were greed, infidelity and poverty, while organizational factors were inadequate staffing, poor internal controls, inadequate training and poor working conditions.

Abdulraheem, Isiaka, & Muhammed (2012) examine the problem of bank frauds and its implications for bank

performance in Nigeria through empirical analysis. The data were extracted from the Nigerian Deposit Insurance Corporation (NDIC) Annual Report from 2004 to 2009 while Pearson Correlation was employed in the evaluation of the data. The study revealed that Nigerian banks recorded the highest fraud cases in 2008 and that, there is a significant relationship between total amount involved in fraud cases and banks profit. On this note the researchers recommended that fraud can be reduced by complying effectively with the policy measures which the government, monetary and supervisory authorities designed to curb the menace of bank frauds in Nigeria.

The effects of internet banking fraud in Nigerian banking industry are felt by all, if not as a customer, then, as a citizen of a nation. The effect of fraud has a chain reaction on the community as a whole because this industry constitutes a vital position in a community. Every part of the economy, especially the banking sector is punctuated with fraud. Thus, its, success or failure goes a long way to determines the success of the community (Gates & Jacob, 2009). Fraud is a major cause of bank failure. The number of internet banking frauds that occurs in Nigeria banks is so alarming with the overall effect on poor bank performance. The amount of money lost to fraudsters is large; such amounts taken out of the coffers of banks do not generate any income for banks, but rather result to bank solvency and liquidity problem (Chiezey & Onu, 2013). Other effects of internet banking frauds include:

1. It destroys the banks reputation.
2. The trust and understanding among staff is reduced.
3. Fraud reduces banks profitability.
4. It discourages banking habit among the banking public.
5. It places emotional and psychological burdens on the fraud victims.
6. The bank ceases to meet up with staff welfare.
7. The bank will lack the ability to compete favorably with its competitors (Eseoghene 2010).

In all, the above studies were carried out on the banking frauds, causes and effects. But, none of the studies were conducted to investigate the sociological analysis of the patterns and effects of internet banking frauds in Nigeria, hence the need for this study.

METHODOLOGY

A deliberate search of literature on sociological analysis of internet banking frauds in Nigeria to identify relevant information on the causes and effects of internet banking frauds was carried out using Google search engine. In addition, utilizing the same Google, the research, also searched and retrieved information from published relevant articles, periodicals and other related internet materials whose subject matter are on the internet banking frauds. Once the key words are typed in the Google engine, several titles, topics and commentaries on the subject of interest propped up while time was taking to open each to select the relevant ones. This was repeated over and over again and days until the required information was accumulated.

Strain theory

Strain Theory was first developed by Robert Merton in 1957 to explain the rising crime rates experienced in the USA at that time. Strain theory has become popular with contemporary sociologists. Merton argued that the cultural system of the USA was built on the ‘American Dream’ – a set of meritocratic principles which assured the American public that equality of opportunity was available to all, regardless of class, gender or ethnicity. The ‘American Dream’ encouraged individuals to pursue a goal of success which was largely measured in terms of the acquisition of wealth and material possessions. People were expected to pursue this goal through legitimate means such as education and work. The dominant cultural message was if you are ambitious, talented and work hard, then income and wealth should be your rewards.

However, Merton (1957), pointed out that these goals were not attainable by all, that the structural organization of the USA mean that the means to get on were not fairly distributed and it was difficult, if not impossible for some to compete and achieve financial success. Merton developed the concept of ‘anomie’ to describe this imbalance between cultural goals and institutionalized means. He argued that such an imbalanced society produces anomie – there is a strain or tension between the goals and means which produce unsatisfied aspirations.

Merton (1957) argued that when individuals are faced with a gap between their goals (usually finances/money related) and their current status, strain occurs. Merton (1957) defined five ways that people adapt to this gap between having a socially accepted goal but no socially accepted way to pursue it.

1. Conformity*:* The majority of people in society choose to conform and not to deviate. They pursue their society's valued goals to the extent that they can through socially accepted means.

2. Innovation*:* Those who innovate pursue goals they cannot reach through legitimate means by instead using criminal or deviant means.

3. Ritualism*:* People who ritualize lower their goals until they can reach them through socially acceptable ways. These "social ritualists" focus on conformity to the accepted means of goal attainment while abandoning the distant, unobtainable dream of success.

4. Retreatism*:* Others retreat from the role strain and reject both society's goals and accepted means. Some beggars and street people have withdrawn from society's goal of financial success. They drop out.

5. Rebellion*:* A handful of people rebel, replacing a society's goals and means with their own. Rebels seek to create a greatly modified social structure in which provision would be made for closer correspondence between merit, effort, and reward.

In relation to subject under discourse, not everyone in our society stands on equal footing. A person may have the socially acceptable goal of financial success but lack a socially acceptable way to reach that goal. For instance, an entrepreneur who cannot afford to launch his own company may be tempted to embezzle/steal from his employer for start-up funds. The discrepancy between the reality of structural inequality and the high cultural value of economic success creates a strain that has to be resolved by some means. As many youth from poor backgrounds are exposed to the high value placed on material success in capitalist society but face insurmountable odds to achieving it, turning to illegal means to achieve success is rational.

This theory was criticized on the ground that it applies only to the lower class as they struggle with limited resources to achieve their goals. Strain theory is still insufficient to explain exactly who will commit crime. Not all people who lack legitimate opportunities turn to crime to do so (Bernburg, 2002).

Fraud Diamond Theory

The theory was first presented by Wolfe and Hermanson in 2004. It is viewed as an expanded version of the Fraud Triangle Theory (FTT). In this theory, an element named capability has been added to the three initial fraud components of the FTT. Wolfe and Hermanson (2004) argued that although perceived pressure might coexist with an opportunity and a rationalization, it is unlikely for fraud to take place unless the fourth element (i.e., capability) is also present. In other words, the potential perpetrator must have the skills and ability to commit fraud. Wolfe and Hermanson (2004), maintained that opportunity opens the doorway to fraud, and incentive (i.e. pressure) and rationalization lead a person toward the door. However, capability enables the person to recognize the open doorway as an opportunity and to take advantage of it by walking through repeatedly. It is further summarized as follows:

1. Capability: This is the situation of having the necessary traits or skills and abilities for the person to commit fraud. It is where the fraudster recognized the particular fraud opportunity and ability to turn it into reality. Position, intelligence, ego, coercion, deceit, and stress, are the supporting elements of capability (Wolfe and Hermanson 2004). Additionally, Giriunas and Mackevicius (2013) noted that, not every person who possessed motivation, opportunities, and realization may commit fraud due to the lack of the capability to carry it out or to conceal it. That this element is of particular importance when it concerns a large-scale or long-term fraud.

Further, that only the person who has an extremely high capacity will be able to understand the existing internal control, to identify its weaknesses and to use them in planning the implementation of fraud. . Similarly, Wilson (2004) discloses that rationalization and capability are all inter-related, and the strength of each element influences the others.

2. Position/Function: The initial factor to enable the fraudster to have the capability to commit fraud is the function or position holding in an organization. Wolfe and Hermanson (2004), state that position and role owned by the employee may perfect his way to breach the organizational trust.

3. Intelligence/Creativity and ego: The fraudster is someone who understands and capable of exploiting internal control weaknesses and using the position; function or authorized access to the greatest advantage (Abdullahi and Mansor, 2015b). Intelligent, experienced, creative people with a solid grasp of controls and vulnerabilities, commit many of today's largest frauds. This knowledge is used to influence the individual's concern for authorize access to systems or assets (Wolfe and Hermanson, 2004:40). The fraudster has a strong ego and great confidence that he will not be detected, or believes that he could easily take himself out of trouble if caught. Such confidence or arrogance can affect one's cost-benefit analysis of engaging in fraud.

4. Coercion, Deceit and Stress: A successful fraudster can coerce others to commit or conceal fraud. A person with a very persuasive personality may be able to convince others to go along with a fraud or to simply look the other way. In addition, it is noted that, a common personality type among fraudsters is the "bully," who "makes unusual and significant demands of those who work for him or her, cultivates fear rather than respect and consequently avoids being subject to the same rules and procedures as others" (Wolfe and Hermanson 2004:41).

The theory was criticized on the ground that fraud diamond is not more qualified as a theory to explain the nature of fraud (Huber, 2016). But the theory provided a profound and clear understanding of the phenomena of internet banking frauds.

Theoretical Framework

For the profound understanding of the phenomena of internet banking fraud in Nigeria, the study adopted strain theory and fraud diamond theory. So to understand the reason or rather in a broader sense, how and why internet banking fraud is entrenching its foot in Nigeria, it is important to do so from the perspective that a couple of social factors or forces join hands together to create the illegitimate opportunity for the fraudster to perpetuate the crime. These social forces can be gleaned from the theories of strain and fraud diamond. In this study two (strain and fraud diamond) criminological theories were integrated. The history of the integrated model approach dates back to the 1940s. It is often described as the pathway through which criminology is seeking to be both as simple and as general as possible. The integrated model perceived law violators as products of interlocking variable or factors (Beirne and messerschmidt, 2000).

First, strain- suggests that individuals turn to deviant behavior when they experience a disjunction between societal goals (e.g., financial success) and legitimate means to achieve them, that is the blockage of the legitimate means and the availability of illegitimate means to goal attainment – is inherent in making people to become a fraudster. In the digital age, exposure to internet wealth (social media, crypto gains, and influencer lifestyles) intensifies perceived financial inadequacy, pushing individuals toward internet banking frauds. Strain provides the motive (financial pressure, frustration, social inequality).

Secondly, the people who perpetrate internet banking fraud are individuals who understand the patterns and are capable of exploiting internal control weaknesses of the system. This is the situation of having the necessary skills and abilities for the person to engage in banking fraud. It is where the fraudster recognized the particular internet banking fraud opportunity and the ability to turn it into reality. This model suggests that those facing strain (strain theory) are more likely to engage in internet banking fraud and who understands the existing internal control and its weakness will use them to commit fraud (fraud diamond theory). Experienced fraudsters with a solid grasp of controls and vulnerabilities, engage in today's largest internet banking frauds.

DISCUSSION OF FINDINGS

The findings of this study were tied around previously reviewed literature, which are on the causes and effects of internet banking frauds. Available literature shows that morbid desire to get rich quick and job insecurity are the major causes of internet banking fraud. These finding is consistent with Asukwo (2009), who stated that the present society is morally bankrupt, little or no premium is put on things like honesty, integrity and good

character. Other causes according to him include: frustration, slow and tortuous legal process, lack of effective deterrent or punishment and at times redundancy on the part of the individual bank to report frauds due to the perceived negative publicity it could create for the image of the institution. Ewa and Odoayang (2012) differed, findings of their study indicated that, internal control design influences staff attitude towards fraud, that a strong internal control mechanism is a deterrent to staff fraud while a weak internal control mechanism exposes the system to fraud and creates opportunity for staff to commit fraud. That most Nigerian banks do not pay serious attention to the life style of their staff members and that most staff members are of the view that effective and efficient internal control design could detect employee fraud schemes in the banking sector.

The study also found that credit card/debit card fraud and identity thefts are two patterns of internet banking frauds which are normally used interchangeably. It involves impersonation and theft of identity (name, social insurance number (SIN), credit card number or other identifying information) to carry out fraudulent activities (Dube, Mashanyanye and Njanike ,2009). Prabovo (2011) also stressed, in order to obtain credit card details, offenders may employ sophisticated methods such as hacking into merchants' databases or simply "engineering" the victims into giving their credit card details or phone calls to bait victims. In an attempt to maximize the benefits from technology utilization most people end up being victims of technology.

However, the effects of internet banking frauds are felt by all, if not as a customer, then, as a citizen of a nation. The effect of fraud has a chain reaction on the community as a whole because this industry constitutes a vital position in a community. Thus, its, success or failure goes a long way to determines the success of the community The above is in line with the position of Dimejesi, (2004) who pointed out that the incidence of fraud is universal and permeates the society as a whole. His study revealed that fraud account for decline in the bank profits, which also agrees with Abdulraheem et al, (2012), the study revealed that Nigerian banks recorded the highest fraud cases and that, there is significant relationship between total amount involved in fraud cases and bank profits. Conversely, Eseoghene (2010) study revealed that, internet banking frauds destroys the banks reputation, reduces trust and understanding among staff, discourages banking habit among the banking public and it places emotional and psychological burdens on the fraud victims. He further suggests the urgent need to secure the systems (banks) to avoid a total collapse.

CONCLUSION AND RECOMMENDATIONS

Internet banking fraud is a big problem in Nigeria. It is a new innovation and the banks efforts in controlling the fraud not effective. Another cause to worry is the materialist value system of the present-day society which encourages all forms of criminality including internet banking fraud. The pattern of internet banking fraud is changing and its effects is better imagined than experienced, reason being that it discourages banking culture and leads to lack of trust among the banking public. However, it can be reduced if not totally eradicated by strengthening bank internal control and adequate technology sensitization especially on internet banking.

The study, however, recommends thus:

1. There is need for the media (both electronic and print media) and religious bodies to promote honesty, handwork, integrity and good character as qualities that determine the reputation ascribe to a person, so that unnecessary competition for acquisition of wealth will be reduced
2. The banking public should not provide personal financial information through phone calls or text messages unless there is a legitimate and assumed reason for that. They should not for instance, throw out old credit cards, drivers' licence, receipts from ATM among other numerous documents which usually have personal data.

REFERENCES

1. Abdullahi, R. & Mansor, N. (2015b). Forensic accounting and fraud risk factors: The influence of fraud diamond theory. The American Journal of Innovative Research and Applied Sciences, 1(5),186-192.
2. Abdulraheem, A., Isiaka, S.B. & Muhammed, A. Y. (2012). Implication of fraud on commercial bank performance. Journal of Accounting, 2(2), 123-129.

3. Adebisi, A.F. (2009). The bankers fortress. Lagos: Mega synergy Nigeria limited.
4. Adeyemo, K. A. (2012). Frauds in Nigerian banks: Nature, deep-seated causes, aftermaths and probable remedies. Mediterranean Journal of Social Sciences, 3(2),35 -42.
5. Adepoju, p. (2014). Nigeria recorded 1,461 cases of electronic fraud in 2014. Retrieved November 20, 2023 from http://www.techcityng.com/nigeria-recorded-1461-cases-of-electronic-fraud-in-2014-nibss/).
6. ACFE, (2007). Report to the nation, occupational fraud and abuse. Austin, TX: ACFE. Retrieved September 28, 2016 from http://www.acfe.com/fraud/report.asp.
7. Akindele, R. I. (2011**) .** Fraud as a negative catalyst in the Nigerian banking industry. Journal of Emerging Trends,2(1),58-65.
8. Asukwo, P. E. (2009, January 23). Bank frauds: A look at the Nigerian banking clearing system, ICAN News, p.19-24.
9. Barker, K.J., D'Amato, J. & Sheridon, P. (2008). Credit card fraud: Awareness and prevention. Journal of Financial Crime,15(4), 398-410.
10. Ballantine ,G.I & Bartlett, H. (2002). Money laundering and international financial crime in small state with special reference to Malta; John Wiley.
11. Beirne, P., & Messerschmidt, J. W.(2000). Criminology, (3rd ed.). Boulder, Colorado; Westview Press.
12. Bernburg, J.G. (2002). Anomie, social change and crime. A theoretical examination of institutional-anomie theory . British Journal of Criminology,42(4), 729–742.
13. Bhasin, M. L. (2013). Corporate governance and forensic accountant: An exploratory study. Journal of Accounting, Business and Management, 20(2), 55-75.
14. Cao, L., Chen, J.W., Li, J., Ou, Y. & Wei, W. (2013). Effective detection of sophisticated online banking fraud on extremely imbalanced data. World Wide Web, 16(4), 449- 475.
15. Cassim, F. (2016), "Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players. School of law, university of South Africa", Based on a paper presented at the First International Conference of the South Asian Society of Criminology and Victimology (SASCV) at Jaipur, India from 15–17 January 2011, pp. 126-138.
16. CBN, (2015). The annual report of Nigeria electronic fraud forum for 2015. Central Bank of Nigeria.
17. Chiezey, U. and Onu, A.J.C. (2013). Impact of fraud and fraudulent practices on the performance of banks in Nigeria. British Journal of Arts and Social Sciences, 3(2), 23-28.
18. Content team (2015) Banking frauds, definitions, cases, examples, processes. Retrieved October 23, 2023 from http://legaldictionary.net/bank-fraud
19. Dimejesi, T. I. (2004). Effective internal control of frauds in banks: A case study of commercial and merchant banks in Nigeria.
20. Dowling, S.& McGuire, M. (2013). Cybercrime: A review of the evidence, Chapter 2: Cyber enabled crimes/fraud & theft, Home Office Research Report 75.
21. Dube T., Mashanyanye, E & Njanike, K. (2009). The effectiveness of forensic auditing in detecting, investigating and preventing bank frauds. Journal of Sustainable Development in Africa,10 (4), 405-425
22. Eseoghene, J. I. (2010). Bank frauds in Nigeria: Underlying cause, effects and possible remedies. African Journal of Accounting, Economics, Finance and Banking Research,16(6), 62-79.
23. Ewa, U. E.& Udoayang, J. O. (2012). The impact of internal control design on banks' ability to
24. investigate staff fraud, and lifestyle and fraud detection in Nigeria. International Journal of Research in Economics & Social Sciences Volume, 2 (2),32-44 .
25. FFA, (2010). Financial Fraud Action report on trend of fraud.Uk. Retrieved, 17, October 2023, http://www.telegraph.co.uk/finance/personalfinance/bank accounts/.html
26. Foley, P. & Jayawardhena, C. (2000). Changes in the banking sector – the case of internet banking in the UK. Internet Research, 10 (1), 19-31.
27. Gates, T. and Jacob, K. (2009). Payments fraud: Perception versus reality. European Journal of Social Sciences, 10(4), 76-82.
28. Gercke, M. (2011). Understanding cybercrime: A guide for developing countries, ICT applications and cyber security division policies and Strategies. Asian Journal of Business Management, 4(2),

232-251.
29. Giriunas, L. and Mackevičius, J. (2013). Transformational research of the fraud triangle. Ekonomika, 92 (4), 150–163.
30. Hermanson, D. R. & Wolfe, D. T. (2004). The fraud diamond: Considering the four elements of fraud. The CPA Journal December 2004.
31. Huber, L.(2016). Crime author of the month. Retrieved from wordpress.com
32. Idolor, E. J. (2010). Bank fraud in Nigeria: Underlying causes, effects and possible remedies. African Journal of Accounting, Economics, Finance and Banking Research, 6 (6),143-152.
33. Idowu, A. (2009). An assessment of fraud and its management in Nigeria commercial banks. European Journal of Social Sciences, 10(4) ,628-640.
34. Ikechi, K.S. & Okay O.E. (2013). The nature, extent and economic impact of fraud on bank deposits in Nigeria. Interdisciplinary Journal of Contemporary Research in Business, 4 (9), 253-265. 1(11), 77-90.
35. KPMG, (2012). Cybercrimes: A financial sector overview, www.kpmg.com/in.
36. Laukkanen, T.(2007). Internet vs. mobile banking: comparing customer value perceptions. Business Process Management Journal, 13 (6), 788-797.
37. Lichtenstein, S. and Williamson, K. (2006). Understanding consumer adoption of internet banking: An interpretive study in the Australian banking context. Journal of electronic commerce research, 7(2), 50-66.
38. Mbelli, T.M. and Dwolatzky, B. (2016), "Cyber security, a threat to cyber banking in South Africa: an approach to network and application security", 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing, pp. 1-6.
39. Mbula, E., Tang, P. and Rush, H. (2013), "The cybercrime ecosystem: online innovation in the shadows?", Technological Forecasting and Social Change, Vol. 80 No. 3, pp. 541-555.
40. Merton, R. K. (1957). Social theory and social structure (rev.ed). New York: Free Press.
41. Miró, F. (2014). Routine activity theory, The Encyclopedia of Theoretical Criminology, pp. 1-7.
42. Nwaze, C. (2008). Bank fraud exposed with cases and preventive measures: Control & surveillance. Associates limited: Lagos.
43. Oladeinde, O. (2017, May 31). Nigerian banks lost N2.19 billion to fraudsters' through electronic platforms in 2016, Premium Times News, p.23-26.
44. Okoye, E.I. & Gbegi, D.O . (2013). An evaluation of the effect of fraud and related financial crimes on the Nigerian economy, Kuwait Chapter of Arabian Journal of Business and Management Review,2 (7),53-74.
45. Oracle, (2012). Fraud fight: Enterprise-wide strategy sets the stage for victory. Oracle Corporation, www.oracle.com.
46. PmnewsNigeria, (2015). The alarming electronic fraud in banks. Retrieved October 20, 2023 from https://pmnewsnigeria.com/2015/05/12/cenbankng.org/the-alarming-electronic-fraud-in-banks/
47. Prabovo, H.Y. (2011). Building our defense against credit card fraud: A strategic view. Journal of Money Laundering Control, 14(4), 371-386.
48. PwC (2016), "Banking in Africa matters – African banking survey", Global Fintech Report, pp. 1-100, [Online], available at: www.pwc.org (accessed October 2023).
49. PwC's Global Economic Crime Survey (2020), "Global economic crime and fraud survey", (7th ed.), pp. 1-32, [Online], available at: www.corruptionwatch.org.za/wp content/uploads/2020/06/ global-economic-crime-survey-20201.pdf (accessed October 2023).
50. Rehman, S. & Siddique, M.I. (2011). Impact of electronic crime in Indian banking sector: An overview. International Journal of Business and Information Technology , 1(2), 159-164.
51. Shinder, D.L. (2002). Scene of the cybercrime: Computer Forensics Handbook. Syngress Publishing.
52. Siong Thye,T. (2002). Money laundering and e- commerce. Journal of Financial Crime, 9 (3), 277-285. Harry Stewart Publications.
53. South African Banking Risk Information Centre (SABRIC) (2019), "Digital banking crime statistics", [Online], available at: www.sabric.co.za (accessed October 2023).
54. Tendelkur, R. (2013), Cyber-crime, securities markets and systematic risk, Joint staff working paper of the IOSCO research department and world federation of exchanges. The strategies they employ in Nigeria. Cyber psychology, Behavior, and Social Networking.

55. Van, N. B. (2017), "An analysis of cyber-incidents in South Africa", The African Journal of Information and Communication, Vol. 20, pp. 113-132.
56. Wilson, D.T. (2004). Understanding the offender/environment dynamics for computer crimes. Information Technology and People,19(2), 170-186.