Internet Payment System, Forensic Accounting and Forensic Investigation: 3M Theory in the Financial Frauds

EFUNTADE, Alani Olusegun, FCIB, FCA.
Afe Babalola University, ABUAD, Ado-Ekiti, Ekiti State, Nigeria.

EFUNTADE, Olubunmi Omotayo, PhD
Federal University Oye-Ekiti, Ekiti State, Nigeria.

DOI: 10.56201/jafm.v9.no7.2023.pg115.130

Abstract
In view of the rapid development in internet payment system and information and communication technology (ICT) that is changing banks mode of payment operations and bringing innovations to banking transactions, and even the method fraudsters operate as well as the likely effects of their activities on the banks and customers if not tackled, this exploratory paper explores forensic accounting, forensic investigation, digital environment, 3M (Manipulation, Misrepresentation, Misapplication) Theory in the Financial Frauds, electronic payment risk management, data mining technique, data matching technique and network security management in internet payment system within banking infrastructures. The paper highlights how forensic accounting and investigation can be employed to resolve the problem of internet and electronic payment fraud and crimes. It is recommended that investigative accounting that will comprehensively entails ICT-related fraud investigation, prevention of fraud and analyzing antifraud ICT-controls in addition to gathering non-financial and financial information should be intensified with modern technology within the banking security infrastructure. There should be fraud control software for financial frauds in digital environment. In today's world where technology has reached a different dimension, sophisticated cases in today's internet banking businesses cannot be revealed by traditional methods and the need for fraud control software against possible negative cases in information environment should be fulfilled in order to eliminate this complexity.

Keywords: *Forensic Accounting; Forensic Investigation; Internet Payment System; digital environment; 3M (Manipulation, Misrepresentation, Misapplication) Theory in Financial Frauds, Data Mining; Data Matching.*

JEL Classification Codes: *M47, M49, E51, G29*

1.0 Introduction

Advancement in technology brought massive innovation in the way and manner banking operations are done in recent times; as the banking operations advanced with technology so also did fraud and fraudulent activities. The importance of putting in place adequate techniques for detecting and preventing fraud in an organization cannot be overemphasis, this among other things lead to the use of forensic accounting techniques in combating fraud in the banking sector. In the context of the development of e-commerce on the Internet, a lot of electronic payment systems have been set up in order to secure online payments. To understand the success of Internet payment systems it is necessary to analyse the strategies of e-commerce actors: consumers, "cyber merchants", managers of networks (telecommunications and payment), suppliers of electronic payment services and banks.

This article investigates also the stakes for the banking environment of the Internet payment systems, forensic auditing and accounting. Forensic accounting can be described as the practice of utilizing accounting, auditing and investigative skills to assist in legal matter and the application of specialized body of knowledge to the evidence of economic transaction and reporting suitable for the purpose of establishing accountability or valuation of administrative proceeding. In wide sense, it can be said to be the integration of accounting, auditing and investigative skills to obtain a particular result (Arokiasamy & Cristal, 2009). Agboare (2021) also defined forensic accounting as the science of gathering and presenting information in a form that will be accepted by a court of jurisprudence against perpetrators of economic crime.

The technology, which takes on different structures and features with each passing day, has left enterprises to interact more with digital environment. While processing the business data in digital environment results in positive outcomes, such as saving on time and costs for businesses, it has also caused a new fraud technique to come into question, which is a negative effect. This technique is called financial fraud. It has led a new profession to come into prominence in financial fraud control performed in digital environment, where 3M theory and competence element play a significant role in the realization of financial fraud. Developments in technology have caused sophisticated cases within businesses to increase and strategic decisions to become more significant, and as a remedy for these causes, allowed forensic investigation reports and forensic accounting to become prominent. In this study, it has been tried to investigate whether core-competencies and characteristics are effective in financial fraud audits in digital environment (Kurnaz *et al.*, 2019).

Bank operations over the years have changed drastically majorly due to developments in the field of information and communication technology and internet payment system. These developments also changed the way fraud and fraudulent activities are perpetuated, and the effect on banking operations. The concerns of stakeholders across all organizations is to seek ways to combat these sophisticated fraudulent activities. The essence of all the measure that organizations adopt is to ensure smoothness of activities, avoid errors (intention and unintentional), detect and prevent fraud and fraudulent practices and discourage those with such intentions.

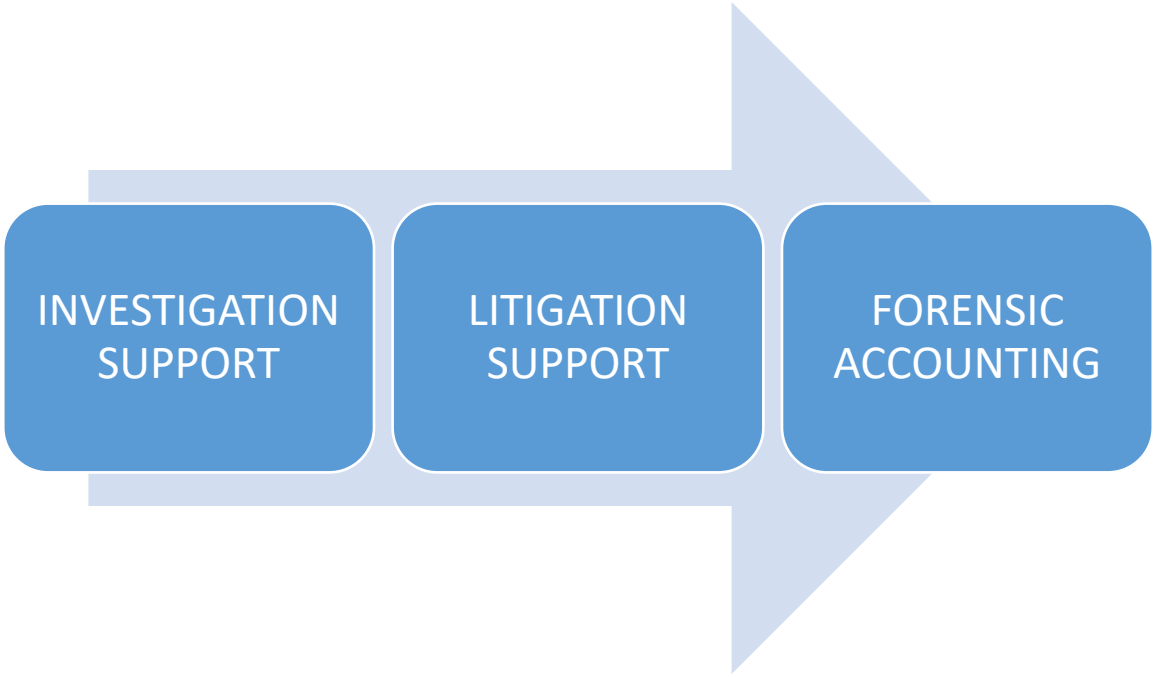

Fig 1: Main Areas of Forensic Accounting

Source: Authors' Conceptualisation, 2023

With the advancement in technology around the globe, there is a massive change in the way banks as well as their customers do business, which place more reliance on the use of electronic medium, the nature of fraud and fraudulent practices has also changed and requires a timely and professional approach to avoid the inherent risk and losses associated with fraud (Agboare, 2021).

Forensic Accounting is the dynamic and strategic tool which helps in combating the corruption, financial crimes, and frauds through the application of forensic auditing techniques such as trend analysis, ratio analysis, CAATs (Computer Assisted Auditing Techniques), Generalized Audit Software, Data Mining Techniques, Forensic analysis of material and electronic evidence (Crain *et al.*, 2019).

2.0 Theoretical Review

2.1 Concept of forensic accounting

Bolgna and Linquist (1995) defined forensic accounting as the application of financial skills and investigative mentality to unresolved issues, conducted within the context of the rules of evidence. Forensic accounting involves the application of accounting and auditing, financial and investigative skills, to unsettled issues, conducted within the context of the rules of evidence (Arokiasamy & Cristal-Lee, 2009; Ozkul & Pamukc, 2012). Following this definition, the focus of forensic accounting is to identify and review fraudulent transactions to identify the real intent of the perpetrator. Such review may take the form of document reviews, interviews, examination of electronic documents, etc.

Dhar and Sarkar (2010) averred that forensic accounting is the application of accounting concepts and techniques to legal problems. It demands reporting where fraud, bribery or embezzlement is established and the report is considered as evidence in the court of law or in administrative proceedings. Arokiasamy and Cristal (2009) opined that forensic accounting is the application of financial skills and investigative mentality to unsettled issues, conducted within the context of the rules of evidence. Enofe *et al.* (2015) are of the view that Forensic accountants provide services in accounting, auditing investigation, damages claims, analysis valuation and general consultation and also have critical roles in divorce, insurance claims, personal damage claims, fraud claims, construction, auditing of publication right and in detecting terrorism by using financial precedence.

Forensic accounting, also called investigative accounting or fraud audit, is a merger of forensic science and accounting. Forensic science according to Crumbley (2005) "may be defined as application of the laws of nature to the laws of man". He refers to forensic scientists as examiners and interpreters of evidence and facts in legal cases that also offers expert opinions regarding their findings in court of law. The science in question here is accounting science, meaning that the examination and interpretation will be of economic information. In the views of Rezaee *et al.* (2006) Forensic accounting is the application of specialized knowledge and specific skill to stumble up on the evidence of economic transactions. It demands reporting, where the accountability of the fraud is established and the report is considered as evidence in the court of law or in the administrative proceeding (Rezaee *et al.*, 2006). Enofe *et al.* (2015) defined forensic accounting as the integration of accounting, auditing, and investigative skills. Simply put, forensic accounting is accounting that is suitable for legal review offering the highest level of assurance and including the now generally accepted connotation of having been arrived at in a scientific fashion (Crumbley, 2006). Bologna (2000) posited that Forensic accounting involves the application of accounting concepts and techniques to legal problem. Forensic accounting has also been defined as the science of gathering and presenting information in a form that will be accepted by a court of jurisprudence against perpetrators of economic crime (DiGabriele, 2009)).

Enofe *et al.* (2015) defined forensic accounting as the process of interpreting, summarizing and presenting complex financial issues clearly, succinctly and factually in a court of law as an expert. Okunbor and Obaretin (2010) added that it is concern with the use of accounting discipline to help determine issues of facts in business litigation. Forensic accounting, if well applied, could be used to reverse the leakages that cause corporate failures; this is because of the fact that forensic accounting is a technique that encapsulates accounting, auditing and investigative skills to address issues relating to financial fraud. It went on to state that the increasing need for forensic and investigative accounting in the banking sector for the complexities of modern-day banking with large volume of complex data cannot be overemphasized (Enofe et al., 2015).

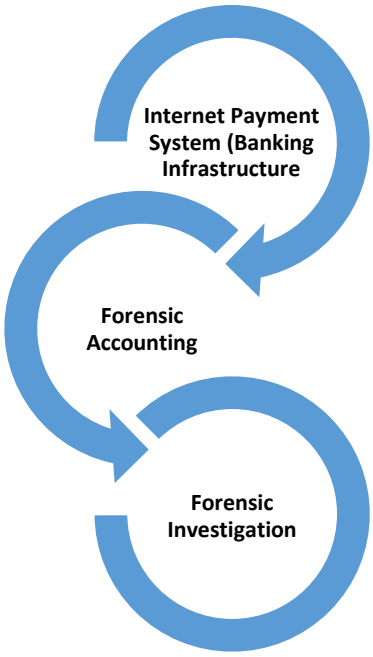

Fig 1: Internet Payment System-Forensic Accounting-Forensic Auditing

Source: Author's conceptualization, 2023

2.2 3M Theory in the Financial Frauds

In order for financial frauds to be performed, existence of certain methods is necessary. These methods are Manipulation, Misrepresentation and Misapplication, which is abbreviated as 3M (Kurnaz et al., 2019). Because today's businesses perform their various transactions online by means of computer software, the profession of forensic accounting that can use the computer experience actively and effectively have taken place. This concept, which is also known as investigative accounting, includes both legal support and investigative accounting. However, the legal support prioritizes the subjects that cause economic damages (Grubor & Simeunovic, 2013). According to the definition by Kurnaz *et al.* (2019), the forensic accounting is to provide an active combination by combining accounting knowledge and research skills in legal support and investigative accounting.

The forensic accounting profession, which have taken place inevitably all around the world, has also triggered a change in the structure of traditional accounting applications. In addition to the front face of the numbers in financial analysis records, it was also tried to take interest in and investigate the background of the numbers (Dayi, 2019). In today's incomprehensible economic structure, this application have become inevitable (Bozkurt, 2000). In the fight against this chaos, it is safe to categorize forensic accountants as 3 different fields of activity and eliminate the chaos, which are stated as Legal Support, Expert's Testimony and Investigation of Fraud, Abuse and Corruption (Okoye & Akamobi, 2009). The investigation of fraud, abuse and corruption is a field of activity which investigates frauds performed in the direction of requests made by business management or owners, or existence possibilities of accounting manipulation. This field of activity aims to reveal, investigate and prevent the frauds and

corruptions performed and to be performed (Crumbly *et al.*, 2011). In the literature, it is called as fraud examination or investigative accounting.

3.0 Responsibilities of Forensic Accounting in Internet payment system

Banking system is the lifeblood and backbone of the economy. Information Technology has become the backbone of the banking system. It provides a tremendous support to the ever - increasing challenges and banking requirements. Presently, banks cannot think of introducing financial product without the presence of Information Technology (Reddy, 2009). Electronic crimes can be of a variety of types such as Telecommunications Piracy, Electronic Money Laundering and Tax Evasion, Sales and Investment Fraud, Electronic Funds Transfer Fraud etc.

In order for businesses to be able to adapt to new business models in recent years, they need tokeep pace with the innovations in computer and communication technology. Innovations in recent years have developed a necessity for digital techniques in order for more data to be collected, stored, processes and turned into information in businesses. As a result of these techniques, developed in businesses, not being applied effectively, there has been an increase in accounting manipulations in businesses. In order to determine and prevent the frauds performed in digital environment by white collars working at businesses, which can be seen in the data, and manipulations performed in compliance with accounting principles and standards, the integrated model in the process of forensic accounting investigation has been developed (Grubor & Simeunovic, 2013). The fact that frauds in businesses are performed by using keyboard much more when compared to frauds by pen or weapon, along with the development of technology, can be evaluated as negative effects of innovations in technology.

Each passing day, the importance of forensic accounting is increasing, which is known as a field that attracts attention due to both its core-competency and characteristics in preventing or detecting these negative effects. Considering the features that separates forensic accounting profession from audit or fraud investigation, which are thought to be among financial fraud determination techniques, it is easily distinguished from other professions as it covers more ground by its nature and performs more detailed investigation.

From the security assessment of Nigerian banks, e-fraudsters had in recent years invaded Nigeria's banking platforms at will, deploying over 185 fake mobile applications on the websites of no fewer than 15 deposit money banks in the country and in the process, extracted customers' personal and financial information with intent to defraud billions of naira from their accounts (Dada *et al.*, 2013). Credit card fraud has become ordinary on internet which not only affects card holders but also online merchants. Credit card fraud can be completed by taking over the account, skimming or if the card is stolen. The term "Internet fraud" refers usually to any type of fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Web sites - to existing fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to broadcast the proceeds of fraud to financial institutions or to other connected with the scheme (Ahuja, 2010).

A forensic accountant should perform the following responsibilities as listed below:

a. Conducting Investigation

Owojori and Asaolu (2009), state that the failure of the statutory audit and the sophisticated financial fraud in recent times had led to the need for forensic audit. Thus, the forensic accountant could be said to have special tools for conducting investigation as to detect and prevent fraudulent activities thereby combating financial fraud. Dada *et al.* (2013) states that a forensic accountant being a fraud investigator is very much likened to a physician who requires significant amount of diagnostic and explanatory work to discover what really is happening. In view of the above, it can be said that a forensic accountant goes beyond the normal audit as to unveil fraudulent activities by using forensic software tools in conducting and investigating transactions and events.

Cabole (2009), states that a forensic accountant does the following: Fraud detection, documentation and presentation in criminal trails and claims; Calculate economic damages, trace income and assets, often in an attempt to find hidden assets or income; Reconstruction of financial statements that may have been destroyed or manipulated; and Expert witness.

b. Analyzing Financial Transactions

Mckittrick (2009) states that a forensic accountant is required to have special skills in inspecting documents for authenticity, alteration, forgery or counterfeiting. Hence, by possessing such skills, the forensic accountant in carrying out his duties can easily detect errors, fraudulent activities and omissions thereby preventing and reducing fraudulent activities. Mckittrick (2009) states that a forensic accountant is responsible for analyzing and identifying the kinds of fraud that could occur and their symptoms.

c. Reconstruction of Incomplete Accounting Records

A forensic accountant in carrying out his function reconstructs incomplete accounting records to settle for example insurance claims, over inventory valuation, proving money laundering activities by reconstructing cash transactions (Owojori & Asaolu, 2009). The above responsibilities listed by Cabole (2009) shows that a forensic accountant must be an expert in financial matters and must have vast knowledge in wider areas which could enable him detect fraudulent activities as soon as one is spot.

Credit and debit card payment with the SSL (Secure Socket Layer) protocol is the most common way of paying on the Internet. An SSL-based transaction assures the encryption and integrity of a transferred message. Merchants can use it in two ways: with or without an intermediary. The version without intermediary (SSLWI) assures message encryption and integrity but exposes both parties to other risks. As a customer communicates their card number and expiry date directly to a merchant, the card number can be illegally used. Moreover, the existence of the merchant is not ensured. The vendor in turn does not have a guarantee that the buyer exists and that they will not repudiate the purchase afterwards. The version with an intermediary (SSLI) assumes the participation of a third trusted party, which guarantees the existence of the vendor as well as denying them access to the buyer's card data. It increases security on the customer's side, assuring them of the merchant's authentication and data confidentiality. Nonetheless, the latter is still not able to identify the buyer. This asymmetry can be eliminated by integrating an electronic signature system into the technology. The electronic signature allows the authentication of the buyer.

An electronic check is the transposition of a traditional check into a dematerialised environment. It uses a digital signature based on key public infrastructure (PKI) that can be automatically verified for authenticity. The customer sends his payment order to a merchant, who presents it to an e-check issuing institution, in order to authenticate it and make the payment. Then, the data related to the e-check is transmitted to a clearing system. The procedure of fund transfer is the same as in the case of a paper check. Similar to the card based system, electronic checks are used for macro-payments but their unit transaction costs are lower. Nevertheless, due to their limited popularity in traditional payments (in fact, used only in the United States and France), they do not constitute a serious threat to card based systems.

E-mail based payments are also used for micro-payments. They are designed for small businesses as well as for P2P (person-to-person) transactions. Online auctions constitute the largest source of e-mail payment revenues. However, they are also used to pay for online gambling and adult entertainment, as well as low-value international payments. As a matter of fact, e-mail payments are not processed via e-mail. E-mails are used for notification, but funds are transferred in the same way banks settle inter-bank transactions. A customer loads an amount of money from his bank account into a service provider account, then specifies the sum of money to be sent and enters the email address of a recipient. Both customer and recipient are notified that the money has been sent. The recipient receives the money and withdraws it from their bank account.

Apart from electronic/virtual wallets and e-mail payments, micro-payments can be handled by incorporating the consumption of a service into phone or Internet billing. Payments included in the phone bill are paid via a telecom kiosk, while Internet bill-based solutions can be operated in Internet service provider (ISP) kiosks and personal account systems. These solutions are very easy to use but they are more expensive than the other micro-payment solutions and have some serious limitations, as they frequently require two telephone lines - lines using ADSL or additional applications. Another solution is based on pre-paid phone and scratch cards but it has just started to be commercially deployed.

Mobile payments are the payments carried out by PTDs (Personal Trusted Devices), such as wireless phones or PDA (Personal Digital Assistant), as well as by other emerging ones such as set-top boxes for interactive television systems or game consoles. Mobile payments can be used for: wireless Internet shopping, face-to-face shopping, vending machines, event and public transport ticketing, P2P (Person-to-Person) payments, pay-as-you-use payments, etc.

Electronic money included three types of payment systems: electronic wallets, virtual wallets and virtual money. Electronic and virtual wallets first require money to be deposited with the manager of the payment system, by various traditional means of payment. Electronic wallets are based on smart card technology, which is used to store data about the customer's funds. Cash is loaded into the e-wallet by a transfer from the cardholder's account. In this way, banks are not involved in the transaction at the moment of purchase. E-wallets mainly target the micro-payment market. At present, they can be used at points of sale, vending machines, parking meters, ticket machines, public payphones, and set-top boxes for interactive TV, etc.

The integration of this system into Internet payments requires a smart card reader on the customer’s side. The simplest and most realistic way to achieve this is to build readers into mobile phones. Such a solution can accelerate the development of pay-per-use services, such as online games,

music, ticketing or mass transit systems. Systems based on the virtual wallet are quite similar to those based on electronic wallets. The only difference is that cash is stocked on the software instead of on a smart card. After having created an account at the system issuer, the buyer only has to enter their ID and password at the moment of transaction. The virtual wallet is used for macro and micro-payments via the internet and virtual money.

3.1 Forensic Investigation Methodology

A special requirement to be prepared in order to collect and store digital evidences for forensic investigations, such as headers in documents, digital evidence type information such as e-mail links and audit logs in investigation, online source information (public records, filing, submissions and court records), information of contacting other experts in case of findings regarding unethical or forceful entries in case of forensic accountants being exposed to assaults, information of rules regarding electronic exploration. Actions to be taken in order to achieve these; to apply rules regarding the storage and management of evidences in an investigation method, to introduce and use a digital evidence in a case scenario, to use the Internet and other sources for investigation and data collection, to define the cases where forensic experts on data security and computers, and to explain the effect of proper use of e-mail on electronic exploration.

Digital Forensic Techniques: Cyber forensics is the process of identifying, analyzing, preserving and presenting electronic evidence in an approach that has legal acceptability in the judiciary. In the technology-driven era, forensic investigation also involves scrutiny of the accounting files and documents, relevant emails, phone logs and hard drives which is the requirement of the modern forensic investigation. Nowadays advanced excel is also used to find out the possibility of fraudulent transactions with the help of Excel Formulae (Eisenberg, 2018).

3.12 Data Mining Techniques

For data mining, there is specific audit software that helps in extraction, classification, clustering of data, regression analysis and retrieval of data. Data Mining helps in the identification of patterns so that new knowledge can be extracted from the information provided to forensic auditors. The historical data available will provide the groundwork for future predictions using data mining techniques.

Forensic investigation is the utilization of specialized investigative skills in carrying out an inquiry conducted in such a manner that the outcome will have application to a court of law. Forensic Investigators are be grounded in accounting, medicine, engineering or some other discipline. Forensic investigation is the examination of evidence regarding an assertion to determine its correspondence to established criteria carried out in a manner suitable to the court. Oyedokun (2015) while discussing the methodology to be followed by fraud/forensic investigators opines that the examination could be approached from both the angels of whether the fraud could have occurred and whether it could not have occurred.

Tactical assessment, which is maybe the most important one, in order to classify and correctly track cyber-crimes, is the necessity of simple knowledge on cyber-crimes and, for intellectual property rights and cyber-crimes, legal knowledge; where, within this scope, it is critical to be able to define the necessary situations for data security or forensic computer experts, and the situations that violate the law, confidential rights and other subjects regarding the crime.

The main necessities in the phase of determination and investigation, which is the last tactical assessment, can be listed as follows: To observe the contradictory statements and attempts of perpetrators in order to cover their active frauds, to affect the regular files with fraud types and to show closeness to electronic files, to seize forensic hardware and write-protectors and deleted files, to acquire software packages according to various information for data extraction analyses. Data mining and continuous supervision and information regarding various software including sound software are suitable for case analyses. General knowledge of techniques and tools, which are used on forensic computers and for recovering files from seized computers, and how forensic accountants should work must definitely be combined with training.

The methodology which he believes that is straight forward as follows (Oyedokun, 2015): Analyzing data which is available; Creating a hypothesis based on such data; Testing the hypothesis and Refining and altering the hypothesis

(a) Analyzing Available Data

This is the most fundamental step as it feeds into the overall investigation and governs whether the fraud auditor would be able to create a hypothesis close to the actual incident. In small investigations involving one or two examiners working on two or three key documents such as agreements, invoices etc. the step cannot be challenging.

(b) Creating Hypothesis

There could be infinite number of hypotheses and it is essential to harness one's imagination and treat only those fitting the merits of the knowledge and information initially available and as learned during performance of documentation analysis.

(c) Testing the Hypothesis

This is the phase where the investigators perform targeted testing of the available documentation and records. They also physical observation of procedures and processes to substantiate or refute their hypothesis.

(d) Refining and Amending the Hypothesis

Targeted testing may expose circumstances which may entirely change the direction of the audit process. This is normal thing and should not cause panic for the fraud auditor. The amendments should be based on the results came from the testing of hypothesis initially developed.

(e) Communicating Results

While reporting the results the auditor should be concise, and deliver the report with concrete facts.

Basing the report on ambiguous evidence would make the report completely useless for the users.

However, a fraud auditor report is distinguished from any other report with one key prominent feature: No fact unsubstantiated. The auditor should make sure that all evidences in the report are clearly organized, catalogued and presented as a support to the fraud report.

3.2 Issues facing computer forensics

The issues facing computer forensics examiners can be broken down into three broad categories: technical, legal and administrative. Technical issues: Encryption; Increasing storage space; New

technologies and Anti-forensics. Forensic accounting techniques are useful in prevention, detection, and deterrence in the area of fraud, money laundering, investigations, crime and terrorist financing (Oyedokun, 2015). These techniques includes, investigative skills, audit skills, legal skill etc. It is now clear that audit, investigation and forensic accounting are much related but they cannot be used interchangeably.

The system should define certain analysis techniques for fraud detection and the analysis defined to state the solution to the difference between an error and fraud; to use computer-based tools for common audit software for data acquisitions (Billing transactions, extraordinary variants, rate and trend analyses, statistical anomalies (Regression, Simulation, Data mining, Pattern recognizing software), to use vertical and horizontal analysis methods, to analyse how the analysts should connect to analysis packages with their laptops; to provide time table theme of analysis packages, to define the situations where forensic computer experts are to be employed, and to explain how the legal transactions are to be carried out and whether the evidences have been collected by a skilled inspector or not (Narveson,2007).

According to Sahut (2008), the greatest deterrent for customers paying via the Internet is the possibility of fraud. Wright (2002) proved that for every $1,000 of Internet business transactions, $1 is still fraudulent6. Then, we have decided to attribute the highest importance to the set of security factors. Having analysed the components of security systems, we have distinguished nine levels of security: identification, confidentiality, authentication, data integrity, customer solvability, non-repudiation, durability, liquidity/convertibility and anonymity/traceability. This distinction is based on already existing research works (Sahut, 2001) and enriched with three additional factors mentioned by Eisenberg (2018). All of the evaluation criteria have been attributed the same relative weight in the composition of the global security score. The only exceptions are the non-repudiation and anonymity/traceability criteria, which are considered a particularly important component of security systems. It is difficult to balance the protection of sellers and the control of personal data use. A great concern of online customers is the possibility of keeping payment activities private and of preventing third parties from observing and tracking spending habits (Eisenberg, 2018).

4.0 Computer Assisted Reviews and Document Review

Computer Assisted Review (CAR) according to Losey (2016) is the review of documents with the assistance of computers and specially designed legal search and review software is a well-established best practice. The term Computer Assisted Review, and the alternative phrase that has the same meaning, Technology Assisted Review, means more than simply reviewing and coding documents on a computer. It is a process where computer software as indispensable tools is used to search and find relevant evidence in a big data setting. The CAR best practices are broken down into these sub-pages: Hybrid Multimodal; Predictive Coding; Bottom Line Driven Proportional Review and Review Quality Controls.

4.1 Data Mining

According to Galvanize (2015), Data Mining is an important analytic process designed to explore data. Much like the real-life process of mining diamonds or gold from the earth, the most important task in data mining is to extract non-trivial nuggets from large amounts of data. Mckittrick (2009) posited that data mining is about processing data and identifying patterns and

trends in that information so that you can decide or judge. Data mining principles have been around for many years, but, with the advent of big data, it is even more prevalent.

Data mining is an interdisciplinary subfield of computer science. It is the computational process of discovering patterns in large data sets involving methods at the intersection of artificial intelligence, machine learning, statistics, and database systems (Christopher, 2010; Trevor,

Robert, & Jerome 2009). The tasks of data mining are twofold: create predictive power-using features to predict unknown or future values of the same or other feature-and create a descriptive power-find interesting, human-interpretable patterns that describe the data.

4.2 Data Matching

Data Matching is the task of finding records that refer to the same entity. Normally, these records come from multiple data sets and have no common entity identifiers, but data matching techniques can also be used to detect duplicate records within a single database (Garcia, 2014). According to Garcia (2014), Data Matching is also known as Record Linkage, Object Identification or Entity Resolution. It is capable of identifying and matching records across multiple data sets is a very challenging task for many reasons. First of all, the records usually have no attribute that makes it straightforward to identify the ones that refer to the same entity, so it is necessary to analyze attributes that provide partial identification, such as names and dates of birth (for people) or title and brands (for products). Because of that, data matching algorithms are very sensitive to data quality, which makes it necessary to pre-process the data being linked in order to ensure a minimal quality standard, at least for the key identifier attributes.

According to Sahut (2008), the nine security criteria are provided below:

1. Identification: in order to initiate a transaction both parties have to be identified: a buyer, who is obliged to pay, and a merchant, who is obliged to provide a product or service. When buyers pay online they cannot use clues from direct observation of the vendor's appearance and behaviour to identify them, as would be possible if they were face-to-face. The same risk applies to the merchants; buyers can acquire goods without paying.

2. Confidentiality: only indispensable transaction details are revealed to the parties, other data remain unknown. For instance, the vendor should not know a customer's card number when an intermediary provides him with a payment certification. The intermediary, in turn, is not supposed to be informed of purchase details. Another problem is to ensure that an unintended third party will not intercept data, as their possible abusive use is the major Internet risk concern.

3. Authentication: electronic transactions have to be authenticated. Honest intentions of trading parties are ensured by the terms of transaction (product features and quantity, price, delivery date etc.). The electronic translation of this contract is the key factor of the future development of electronic commerce. Customers require a guarantee that a merchant will not charge them for an imaginary purchase.

4. Data integrity: during the session, payment data cannot be intentionally or unintentionally tampered with.

5. Non-repudiation: merchants want to be sure that the payment obligation will not be repudiated afterwards.

6. Customer solvency: customer solvency can be verified by a merchant or, to a certain extent, guaranteed by a bank.

7. Durability: users want to be sure that their data or transaction details can be verified and are not going to be misused after a certain period of time. The transaction system has to be resistant to any hardware or software defaults.

8. Liquidity/convertibility: transferred money can be withdrawn or converted to another currency immediately, without any additional procedures.

9. Anonymity (Privacy): anonymity (or privacy) refers to a customer's ability to do a transaction on the Internet, without her/his identity being known. When a credit card is used, the user needs to be identified in order to have a secure payment. But customers want to be anonymous to the merchants and prefer not to leave any traces of completed transactions.

5.0 Conclusion and recommendations

In view of the rapid development in internet payment system and information and communication technology that is changing banks mode of operations and bringing innovations to banking, and even the method fraudsters operate as well as the likely effects of their activities on the banks and customers if not tackled; and in consideration of the findings of this study that forensic accounting has a significant effect on fraud detection, the research made the below recommendations: More forensic accountants and investigators should be employed and trained, considering the growing relevance of forensic accounting techniques in curbing modern day fraud and financial crime in internet payment system brought about by advancement in technology, changes in the modus operandi of banks in developing economies and in line with the findings of this study that revealed that forensic accounting components are effective in electronic fraud detection.

Cyber forensics has revolutionized the scope of forensic accounting. There are various techniques such as benchmarking, ratios analysis, specialist software, system analysis, etc, which can be employed beforehand to curb the malpractices of companies. Due to the increasing number of scams in in the world of internet payment, it is the need of the hour to have forensic professionals to handle the cases of financial frauds and scams.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

Authors' contributions: All authors contributed, read and approved the final manuscript.

References

Agboare, E. I. (2021), Impact of forensic accounting on financial fraud detection in deposit money banks in Nigeria. *African Journal of Accounting and Financial Research, 4*(3), 74-119.

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

Arokiasamy, L., & Cristal-Lee, S. (2009). Forensic accounting: public acceptance towards occurrence of fraud detection. *International Journal of Business and Management*,145-160

Bolgna, G. & Linquist, R. (1995). *Fraud Auditing and Forensic Accounting: New Tools and Technique. 2ndEd*. New York, NY: John Wiley & Sons.

Bologna, J. (2000). The 'one minute fraud auditor' Revisited. *Forensic Accounting Review*,*12*(12),1-4.

Cabole, C. (2009). Forensic accounting: A paper presented at the (Hilton Hotel Lagos), *Certified Public Accountant Journal*. New York. Retrieved online.

Christopher, C. (2010). Encyclopædia Britannica: Definition of Data Mining. Retrieved from http://www.britannica.com/EBchecked/topic/1056150/data-mining

Crain, M. A., Hopwood, W. S., Gendler, R. S., Young, G. R., & Pacini, C. (2019). *Essentials of Forensic Accounting*. John Wiley & Sons.

Crumbley, D. L. (2005). *Qualifying as an Expert Witness*. In Walter J. Pagano and Thomas A. Buckhoff, eds., Expert Witnessing in Forensic Accounting, Philadelphia: Edwards.

Crumbly, D. L., Lester E., H. & Stevenson, S. (2011). *Forensic& Investigative Accounting, 5th edition*.

Dada, S. O., Enyi, P. E., & Owolabi, S. A. (2013). Forensic accounting: A relevant tool for effective investigation of bribery cases in Nigeria. *Unique Journal of Business Management Research,1*(5), 96-99.

Dada, S. O., Owolabi, S. A. & Okwu, A. T. (2013). Forensic accounting a panacea to alleviation of fraudulent practices in Nigeria. *International Journal of Business, Management and Economics Research, 4*(5),787-792.

Dada, S. O., Owolabi, S. A., & Okwu, A. T. (2013). Forensic accounting: A panacea to alleviation of fraudulent practices in Nigeria. *International Journal of Business Management Economics Research,4*(5), 787-792.

Dayı, F. (2019). Net İşletme Sermayesinin Likiditeye Etkisi: BİST 30 Şirketlerinde Uygulama. *KOCATEPEİİBF Dergisi, 21* (1), 47-58.

DiGabriele, J. A. (2009). Fishbowl the forensic accountant: A closer look at the skills forensic accounting education should emphasize. *The Forensic Examiner ,18* (2), 77-79.

Efiong, E. J. (2012). Forensic accounting education: An exploration of level of awareness in developing economies - Nigeria as a case study. *International Journal of Business and Management, 7* (4). 26-34.

Effiok, S. O., Ojong, C. M. & Usang, O. U. E., (2012). The implication of occupational fraud and financial abuse on the performance of companies in Nagger'. *Interdisciplinary Journal Of Contemporary Research In Business, 4*(7),516-533.

Eisenberg, P. (2018). Application of the net worth method in forensic accounting investigations. *International Research Journal of Multidisciplinary Studies,4*(10), 1-23.

Emeh, Y. & Obi, J. O. (2013). An empirical analysis of forensic accounting and financial fraud in Nigeria. *African Journal of Social Sciences, 4,* 112-121.

Enofe, A. O., Agbonkpolor, O. R. & Edebiri, O. J. (2015). Forensic accounting and financial fraud. *International Journal of Multidisciplinary Research and Development, 2*(10), 305-312.

Enofe, A.O., Idemudia, N.G. & Emmanuel, G. U. (2015). Forensic accounting a panacea to fraud reduction in Nigeria firms. *Journal of Accounting and Finance Management,1*(6),1-31.

Enofe, A. O., Okpako, P. O. & Atube, E. N. (2013). The impact of forensic accounting on fraud detection. *European Journal of Business and Management, 5*(26), 61-73.

Enofe, A. O., Utomwen, O. A. & Danjuma, E. J. (2015). The role of forensic accounting in mitigating financial crimes. *International Journal of Advanced Academic Research*,1-25.

Garcia, R. I. (2014). *What is Data Matching*? Retreived from https://infosimples.com/en/articles/what-is-data-matching

Gbegi, D. O., & Adebisi, J. F. (2014). Forensic accounting skills and techniques in fraud investigation in the Nigerian public sector. *Mediterranean Journal of Social Sciences,5*(3), 243-252.

Grubor, G. R. & Simeunovic, N. (2013). Integrated forensic accounting investigative process model in digital environment. *International Journal of Scientific and Research Publications,3*(12),1-9.

Hopwood, W. S., Leiner, J. J. & Young, G. R. (2008). *Forensic Accounting*. New York: McGraw-Hill/Irwin.

Kosmas, N., Thulani, D., & Edwin, M. (2009). The effectiveness of forensic auditing in detecting, investigating, and preventing bank frauds. *Journal of Sustainable Development in Africa,10*(4), 405-425.

Kurnaz, N., Köksal, I. & Ulusoy, T. (2019). Forensic accounting in financial fraud control in digital environment: A research on independent auditors. *Turkish Studies, 14*(3), 1609-1627.

Losey, R., (2016). *Computer Assisted Review: Electronic Discovery Best Practices*. Retrieved from http://www.edbp.com/search-review/computer-assisted-review/

Malphrus, S. (2009). Perspectives on retail payments fraud. *Economic Perspectives, 33*(1),31-36.

Mckittrick, C. (2009). Forensic accounting- it's broader than you might think and it can help your Organization. *Forensic Accounting,1*,1-3.

McMahon, R., Serrato, D., Bressler, L. & Bressler, M. (2015). Fighting cybercrime calls for developing effective strategy. *Journal of Technology Research,6*,1-15.

Moore. T, Clayton. R & Anderson. R (2009). The economics of online crime. *Journal of Economic Perspectives, 23* (3) , 3-20.

Narveson, S. D.(2007). Education and training in fraud and forensic accounting: A guide for educational institutions, stakeholder organizations, faculty and students. *West Virginia University, February*,1-70.

Okoye, E. I. & Akamobi, N. L. (2009). The role of forensic accounting in fraud investigation and litigation support. *The Nigerian Academic Forum,17*(1),39-44.

Okunbor. J. A & Obaretin, O. (2010). Effectiveness of the application of forensic accounting services in Nigerian corporate organizations. *AAU Journal of Management Sciences, 1*(1), 12-23.

Owolabi, S. A., Dada, S. O., & Olaoye, S. A. (2013). Application of forensic accounting technique in effective investigation and detection of embezzlement to combat corruption in Nigeria. *Unique Journal of Business Management Research,1*(4), 65-70.

Oyedokun, G. E. (2015). Integrity of financial statement and forensic accounting techniques in internal control of business organisations; being post-field Thesis presentation to the department of Accounting of Babcock University for in partial fulfillment for the award of Master of Science Degree (MSc.) in Accounting on March 31, 2015.

Özkul, F. U., & Pamukçu, A. (2012). *Fraud Detection and Forensic Accounting. In Emerging Fraud*. Springer Berlin Heidelberg.

Reddy, G. N. (2009). IT- based banking services enhancing efficiency. *Financial Analyst, 69* (11),34-46.

Rezaee, Z., Crumbley, D. L. & Elmore, R. C. (2006). Forensic accounting education: A survey of academicians and practitioners. *Journal of Forensic Accounting,10*(3),48-59.

Saddique, I & Richman, S. (2011). Impact of electronic crime in Indian banking sector. *International Journal of Information Technology,1*,159-164.

Sahut, J-M. (2001). Les paiements électroniques sur Internet. *Gestion 2000*, Mars-Avril.

Sahut, J. M. (2008). Internet payment and banks. *International Journal of Business, 13*(4),362-376.

Wright, D. (2002). Comparative evaluation of electronic payment systems. *INFOR,40*(1),71-85.