

FORENSIC BACKGROUND INVESTIGATION TECHNIQUE AND INSIDER FRAUD THREATS: EVIDENCE FROM THE LOW-LEVEL SUPPLY CHAIN FIRMS IN NIGERIA

Damilola Gabriel Fagboro^a, Omowunmi Jumoke Ogunleye^b, and Adegbola Olubukola Otekunrin^c

^aDepartment of Accounting, University of Lagos, dfagboro@unilag.edu.ng

^bDepartment of Accounting, University of Lagos, oogunleye@unilag.edu.ng

^cBowen University, Iwo, Osun State, Nigeria, otekunrin.adegbola@bowen.edu.ng

^aCorresponding Author: dfagboro@unilag.edu.ng

Abstract

The paper explores the nexus between forensic background investigation techniques on employees and insider fraud threats in Nigeria's low-level supply chain firms. The research design adopted for the study is a survey. Primary data are gathered from the 109 volunteered sole-business owners used for the analysis; descriptive and inferential statistical tools are deployed to analyse the data. Findings reveal that sole-business owners rarely conduct background investigations on their employees during recruitment. The background intelligence gathering among the firms' employees is significantly low. Slack employment policies, misplaced trust, and uncoordinated internal control systems among the firms mostly create avenues for employees to commit fraud. The study concludes that both tactical and strategic approaches to intelligence gathering on employees are suitable methods to build up a detailed signal of threats to a business. Initial assessments and background forensic investigation processes on employees help make timely decisions about how to respond to insider fraud threats and identify what protective measures to take. The study recommends that sole business owners protect their investments by employing trustworthy persons, ensuring the safety of the assets, and upholding the reputation of the firm's image. Pre-employment and on-the-job forensic background investigation techniques and tactical intelligence evaluation on the employees should be part of the standard anti-fraud strategies of a small-size business firm. Credibility in the information gathered, and intelligence products generated by each employee must be a hallmark of the employing firm.

Keywords: *Forensic investigation, intelligence gathering, employees' fraud threats, and supply chain firms.*

1. INTRODUCTION

Globally, on-the-job fraud threats are a complex problem for the management to deal with in a workplace environment. This incidence of abuse of trust among the employees has raised a question on the need for business owners and managers to incorporate more effective methods of fraud detection, investigation, resolution and prevention. Extant studies on workplace fraud risks have explained fraud as the interaction of three causal influences affecting a pre-planned perpetrator (Cressey, 1953; Albrecht, 2014; and Homer, 2019). On this strength, Cressey (1953) identified three fraud elements as: situational pressure, opportunity to commit the fraud, and ability to rationalize (personal attitude). Following up on the Cressey's submissions, Albrecht (2014) maintained that neither the pressure nor the opportunity has to be real before an employee commits fraud. Homer (2019) agreed with the positions of both Cressey (1953) and Albrecht (2014) that the elements of fraud risk factors must be all present to effectively actualise fraud in a workplace environment. However, studies in social psychology suggest that business owners and managers mostly rely more on attitude cues when explaining or predicting an employee's criminal tendencies (Coenen, 2009; PBL Blackwell, 2010). To this end, the social psychology study categorised explanations for insider fraudulent threats as either 'dispositional' or 'situational' (Ramamoorti, Morrison III, Koletar, and Pope, 2015). Against this background, causal factors attributable to an employee's internal attitude are classified as dispositional; while those that are part of the person's external environment (for instance, opportunity and incentive) are considered situational (Ruankaew, 2016; Peprah, 2018).

Stated in a generic term, 'fraud' incorporates a wide range of criminal conducts characterised by deliberate deception, concealment and violation of trust in order to obtain unfair, unjustified or unlawful gain, detrimental to the victim (Homer, 2019). The unpleasant consequences of business fraud risks are not only to individuals, families, entities, and community; but also on national economic systems (PBL Blackwell, 2010). Evidence has been provided that insider frauds could lead to financial ruin of a family and community, enterprises as well as seriously damage economic systems (Blackwell, 2010). Not few sole-business owners would argue that there are sufficient internal controls in place to prevent, or eliminate fraudulent actions. On the contrary, studies have shown that conservative management internal control measures do not entirely avert fraud occurrence (Marks, 2012; Ruankaew, 2016). According to Said, Alam, Ramli, and Rafidi (2017), one of the challenges of detecting, investigating, resolving and preventing employee fraud is that there are so many manifests of fraud that require different methods to solve. Over the years, studies on occupational financial fraud has been documented as a direct response to the changes in the society, such as technological advancement (The Chartered Institute of Management Accountants (CIMA), 2009; Bichanga, 2019). The Association of Certified Fraud Examiners (ACFE) (2018) reported that the cost of employee frauds to small scale businesses could be difficult to estimate because not all frauds are discovered; not all discovered frauds are reported; not all discovered frauds are investigated; and the management would not always pursue legal actions in the quest to avoid negative public image.

In its report, the International Academy of Forensics (IAF) (2019) concluded that despite significant advances in fraud detection, investigation, treatment and prevention methods; fraudulent activities among employees continued to be a source of grave threats to the survival of

many low-level (small scale) businesses. The cost of low-level business fraud on the economy is at an astounding degree (Ruankaew, 2016). Langner (2010) reported that small scale businesses were especially vulnerable to insider frauds than the bigger ones; the larger businesses have financial capacity to engage full-time professional fraud examiners. On the contrary, as a result of the paucity of official on-the-job fraud data base, it appears that there are no statutory documented figures on the total cost of workplace fraud threats in low-level firms in Nigeria. Besides, a good number of the previous studies on corporate crime focused mainly on large firms; whereas employee frauds are a fact of life in the modern low-level workplace (The National Research Council, 2000; Marks, 2012). In effect, this paper argues that much that has been said about the fraud risk management of big business is presumed to apply as well to smaller enterprises. On the contrary, the small-scale firms have their own peculiar problems, which must be solved and handled in ways specifically applicable to them.

Consequently, the current paper theorises that the existing convectional internal control measures might no longer be as effective as when they were initially proposed. Besides, not much empirical evidence in low-level businesses has been collected in the context of developing economies, such as Nigeria; especially in the area of fraud committed by employees (Okaro and Okafor, 2013; Yekini, Ohalehi, Oguchi, and Abiola, 2018). Individually, these fraudulent activities are rarely significant enough to warrant engaging professional fraud examiners, but if left unchecked; small crimes add up to big losses. In enterprises without resident fraud investigators; fraud risk management mostly fall to the business owners. The current study postulates that businesses change; and as they do, more/different employees are engaged for old and newly created positions. On the basis of this analogy, this study argues that a good number of the prior studies on fraud mitigation did not consider forensic employment background investigation as a veritable tool to mitigate insider fraud threats in a workplace environment. Consequently, this study is an attempt to provide a forensic framework for investigating the background of employees as an emerging strategy to address fraudulent activities in low-level supply chain firms, having Nigeria in focus.

2. LITERATURE REVIEW

The Theoretical Framework

In the history of forensic accounting investigation research thoughts, some theories on employee fraud causation have been formulated, and still being proposed. Till date, notably among these theories are: Differential Association Theory developed by Sutherland (1939); Fraud Triangle Theory propounded by Cressey (1953); Fraud Diamond Theory proposed Wolfe and Hermanson (2004); and **Fraud Pentagon Theory postulated by Marks (2012)**.

Against this background, it could be opinionated that each succeeding fraud theory is both an offshoot and explanation of the previous. Of these, the Theory of Fraud Triangle propounded by Donald Ray Cressey in the year 1953 stands the test of time as it continues to be as influential in the contemporary society as it was when first proposed (Albrecht, 2014; Homer, 2019). Cressey's research in the early Nineteen Fifties provided strong insight into the question: '*why fraud is committed?*' Of which was the result presented in what is known as the 'fraud triangle'. As documented, Cressey interviewed 200 fraudsters who were serving various terms indifferent correctional centers. According to Cressey, the corporate fraudsters were convicted of embezzlement in their respective places of work. One of the major conclusions of Cressey's

research efforts was that every fraud had three things in common (fraud causal conditions or explanations). These elements are identified as: Pressure (motivation/incentive), Rationalisation of personal ethics / integrity, and Knowledge of Opportunity to commit the Financial Fraud.

These three determinants are adduced as the corners of the Fraud Triangle Theory. Historically, these elements of business fraud were first identified by Sutherland in the year 1939; and subsequently developed by Cressey in the year 1953. Later, Albrecht, et al. (1982) adapted the concept from Criminology to Accounting; and reinforced the decomposition with a review of over 1,500 references on fraud. The authors identified 82 fraud-related variables which they combined into three forces (branded '*red flags*'). These forces influence the decision to commit or not to commit fraud (Akuh, 2017). Langner (2010) submitted that the **theory** of fraud triangle provided a useful framework for business owners to evaluate their vulnerability to insider frauds and related workplace wrongdoings. Thus, the theory is useful in predicting who is more likely to commit fraud and the circumstances under which business fraud is considered more probable. The postulations of the fraud triangle theory can help sole business owners focus on their anti-fraud policies. Consequently, this paper is premised on the Fraud Triangle **Theory** as propounded by Donald Ray Cressey in 1953.

An Overview of a Supply Chain Business

A supply chain has been explained as a network between a merchandizing firm and its suppliers to produce and distribute a specific product(s) or service(s) (Blanchard, 2010). The firms involved in the supply chain have been identified as producers, vendors, warehouses, transportation companies, distribution centers, and retailers. The functions in a supply chain include product development, marketing, operations, distribution, finance, and customer service (The National Research Council, 2000). These functions include product development, marketing, operations, distribution networks, finance, and customer service. Further, a low-level supply chain business is a small-scale business (Blanchard, 2010). Against this background, this study is on employee fraud threats in low-level supply chain firms in Nigeria. These firms consist both the upstream and downstream elements of supply-chain management (SCM). Akuh (2017) had reported that small scale businesses were more prone to employee fraud, unlike bigger businesses.

Insider Fraud Threats in a Context

Okaro and Okafor (2013) carried out a study on the effectiveness of fraud risk management using the micro finance banks in Nigeria, by undertaking extensive review of literature in the field of study. On the basis of the analysis of data used for the study, the outcome identified some key drivers of financial frauds mostly committed by employees in a workplace environment. These critical factors of fraud were weak internal control systems, unethical management and board practices, frail regulatory institutions, undeterred perpetrators' greed, ineffective internal and external audit functions, and a business environment that extols wealth irrespective of how it is made. Given the peculiar environment circumstances in Nigeria, Okaro and Okafor recommended the following holistic approach to mitigate employee frauds: whistleblowing legislation, and introduction of forensic accounting to checkmate fraud in the micro finance institutions in Nigeria.

Omar, Nawawi and Salin (2016) conducted a study to investigate the major causes and impact of employee fraud on business organisations, focusing on the automotive industry. Qualitative data

analysis was adopted to carry out the study. The authors adopted two different techniques to gather data for the study. First technique was the content (document analysis) on various reports, such as employee fraud reports and records of disciplinary action; while the second technique was a series of interviews with employees from different levels and various departments of the automobile company used for the study. On the strength, the outcome of the study reveals that the most popular type of fraud was misappropriation of assets, including theft of cash and inventories. No significant differences were seen in terms of fraudster's position, as they can come from both the lower and the management levels. However, Omar, Nawawi and Salin observed that majority of the fraudsters came from the operational and sales departments. The study concluded that motivations to commit fraud included lack of understanding about fraud behaviour, opportunity to commit fraud and lifestyle and financial pressure. The authors recommended that closed supervision, fraud awareness training, clearer job descriptions, cultivation of a pleasant working environment and improved security control. The study provided further confirmation of both the fraud triangle and fraud diamond theories on the causes of the fraud. The study is consistent with the findings of the prior surveys conducted by CIMA, 2009.

Grounded on the Fraud Triangle Theory, Akuh (2017) conducted a survey on small retail business strategies to detect and prevent frauds committed by employees; The study explores strategies used by selected managers and owners of small retail businesses to detect and prevent employee fraud. Ten voluntary participants from five small retail businesses participated in the study. Further, nine firm owners/managers participated in a face-to-face semi-structured interview, and one participated in a telephone interview. These participants included five owners and five managers of small retail businesses in the state of Michigan in the United States of America (USA). These group of participants had implemented strategies to detect and prevent employee frauds. Besides, the author gathered additional data through semi-structured interviews; which entailed a process of methodological triangulation, casual observations and documentary evidence. On the basis of thematic analysis through coding narrative segments, the outcome of the study included themes of controls and communication, cash register accountability, segregation of duties, monitoring, and action against perpetrators. In terms of policy implementation, the findings of the study have the ability to counter employee fraud in a workplace environment. Nevertheless, the implications of Akuh's (2017) study may not be totally applicable to the developing economies because of their environmental peculiarities.

Peprah (2018) conducted a study on the predictive relationships among the elements of fraud diamond theory; and how the relationships were ranked for early detection of fraud. The author adopted ranking Likert scale questionnaire on the four elements of fraud diamond, which are pressure, opportunity, rationalisation and capability to commit fraud. The study found positive linear relationships among all the four elements of the fraud diamond theory, and concluded that if opportunity could be minimized, potential fraudsters' capability would be rendered redundant through supervision. Also, if rationalisation could be made difficult, potential fraudsters would delay or avoid their act of fraud. The author recommended that: Policies that would reduce the opportunity to commit fraud and rationalisation should be given much attention. Effective supervision should be intensified to control capability, which supported previous research on fraud risk management that of all the elements of fraud, opportunity is the dominant factor.

Zuberi and Mzenzi (2019) explored the fraud factors propelling occurrences of both employee and management fraud in the risk context of Tanzania, as a developing economy. The authors developed and administered a survey instrument to 114 participants who had witnessed, or examined, or been involved in fraud resolutions. The participants used for the study consisted business managers and owners, fraud victims, fraud examiners, financial auditors, legal practitioners, and law enforcement agents. The study identified six factors that were responsible for employees and managers engagement in fraudulent activities. These factors were social incentives, business financial strain, and pressure, greed, internal pressures, operating problems, and malevolent work environment. In addition, Zuberi and Mzenzi (2019) found that fraudsters rationalized their behaviours through five significant neutralisation techniques identified as attitude, denial of injury, social weighting, transferring of blame, and prior fraud history. Victim organisations were identified to have three main fraud opportunities: poor control environment, inadequate control activities, and circumstances that allowed collusive behaviour among fraudsters. The authors, therefore, concluded that business managers/owners and anti-fraud professionals should acknowledge the factors responsible for fraud occurrences, with intent to put in place measures to prevent the frequency of fraud losses.

From the review of prior studies on financial fraud in a workplace environment, it could be argued that the authors did not cover aspects of forensic background investigation and tactical intelligence gathering as part of anti-fraud strategy. This is the observed gap in knowledge this paper intends to address.

Forensic Background Investigation on Employees

Forensics (*used with a singular verb*) means application of science and technology principles and methods to carry out a detailed investigation in both criminal and civil matters, with a view to establishing incontrovertible facts/evidence for the benefit of the end users (IAF, 2019), and forensic investigation deals with the study of physical evidence in a modern legal context. Bohan (2010) posited that the reports of the forensic investigation must be valid, reliable, true, timely and credible. According to Chatman (2009), the main purpose of forensics is to remove doubts by establishing indisputable evidence / facts in both civil and criminal matters. Forensics covers two broad areas of operation, namely: Investigation and Intelligence Gathering. Forensic operations could either be overt (open) or covert (secret), or a combination of both, depending on the type of engagement on hand (IAF, 2019). Forensic investigation emerged because the existing traditional crime investigative and preventive methods have been virtually rendered obsolete and ineffective (Bichanga, 2019). Hence, this paper proposes forensic investigation and intelligence gathering on employees as strategies to prevent insider (on-the-job) fraud threats.

Reasoning from the perspective of fraud risk management as a key factor to a business success, Suponcic (2017) explained a background investigation as a process a person or organisation adopted to confirm a personality's identity claims. In this instance, background investigation is an avenue to know a person's criminal record, education background, employment history and other activities that happened in the past in order to confirm their validity (Adu, 2018). Employers conduct background investigation to avoid hiring someone who may pose a threat to the workplace or become a liability to the organisation (Levashina and Campion, 2009). Suponcic (2017) identified the basic areas mostly covered by background investigations as: Education background; professional qualification(s); employment history; biometric data; criminal records; financial standing; trade union activism; medical screening; political views/affiliations; drug and alcohol

testing; and social media. Small (2015) concluded that it was standard practice for employers to carry out background investigations on applicants.

On the strength of the analogy, this paper proposed two hypotheses, namely: There is no significant relationship between forensic intelligence gathering technique on employees and insider fraud threats amongst low-level supply chain business in Nigeria; secondly, that there is no significant relationship between forensic background investigation on employees and insider fraud threats amongst low-level supply chain business in Nigeria.

3. METHODOLOGY

Research Design

The research design for this study is a survey; it involves electronic collection of opinions from the volunteered respondents used for the study.

Research Population and Sample

The population of the study is 119 volunteered sole business owners of low-level supply chain firms operating in Nigeria. They were severally contacted through their respective online (social media) platforms. Only the business owners are involved in the study, because previous studies have provided evidence that managers commit fraud against their employers (CIMA, 2018; ACFE, 2018; Zuberi and Mzenzi, 2019). According to Ignou (2012), this method of research population selection is adopted in cases where the specialty/position of the respondents will bring more accurate, reliable and valid results than by using the whole target population. Creswell (2012, p.9) noted that this “method of population selection is considered a viable option in obtaining data from a very specific group of people, when a limited number of individuals possess the trait of interest”. Thus, the method of sample selection is considered the most suitable as it provides avenues to address the research questions designed for the study and the tests the hypotheses postulated.

Further, due to the relatively small size of the population, the study adopts the entire research population as its research sample. Lucas (2014, p.107) positioned that “The only time a researcher relies on sampling techniques is when testing all the individuals in the population is impossible”. Creswell (2008) maintained that “the ideal scenario is to test all the individuals to obtain reliable, valid and accurate results”. According to Lucas (2014) population could be wholly adopted as a sample size.

Procedure for Data Collection

The primary data source consisted of a set of designed questionnaire administered to one hundred and nine (109) volunteered sole business proprietors of low-level supply chain firms operating in Nigeria. Besides the main respondents; ten (10) copies of the questionnaire were initially used for pilot study. All the volunteered respondents (109) filled and returned the questionnaire through the same electronic medium with which the survey instrument was administered.

Based on the initial assessment of the responses of the respondents in the returned questionnaire, oral interviews (through telephone conversation) were scheduled and conducted using 32 of them (the respondents). This approach was considered appropriate on the bases of the extent of insider fraud threats the respondents disclosed they had experienced in their respective businesses. The

respondents were required to provide detailed explanations on how the frauds were perpetrated, discovered, investigated, and dispensed with; and efforts made to mitigate future occurrence. The outcome of the interview was incorporated as part of the findings in this paper.

Research Instrument

A set of structured and validated questionnaire was developed for the study. The questionnaire consisted of five sections with alphabetical numbering (Sections) A to E. Section A was Demographic Data, Sections B to D contained five-point Likert scale items, and while Section E consisted of ranking eight (8) anti-fraud strategies. Furthermore, items measuring various variables were interspersed (Ignou, 2012). Following the guidelines provided in Dutta (2013), the survey instrument was designed using opinion, factual items or categorical questions as well as open-ended items. The Likert five-point scale was adopted for opinion items. The instrument underwent and passed both validity and reliability tests.

Methods of Data Analysis

This paper adopted both descriptive and inferential statistics to analyse the data. Two hypotheses were designed to achieve the objectives of the study. Both hypotheses were tested with Pearson Correlation analysis (at $\alpha = 0.05$).

4. DATA PRESENTATION AND ANALYSIS

Job Position Pattern of the Respondents

All the one-hundred and nine (109) respondents for this study are sole owners and full-time directors of their respective firms. Thus, the respondents are deemed to possess first-hand data, knowledge and experience of the organisations under study.

Ranking of Implementation of Anti-Fraud Strategies

Table 1 shows the result of the extent in which the respondents incorporate any of the eight (8) commonest anti-fraud strategies, in their respective firms. Each respondent was required to do rankings based on their respective personal expertise and experience as a sole business owner and employer of labour. Each participant was asked to rank (from 8 to 1) the measures in order of their application in their respective businesses. The respondents were informed to assign '8' points to the most applied strategy, '7' points to the strategy that is next most used, and '1' to the least applied strategy. Thus, the most applied anti-fraud strategies have the highest mean scores; while the least applied strategies have the lowest mean scores.

Table 1: Mean Ranking of the Perceived Application of Anti-Fraud Strategy

Item	SS	Mean Score	Ranking	Significant Level
Internal control mechanism.	109	4.1825	1 st	Very High
Established fraud policies.	109	3.7293	2 nd	High
Good reward system.	109	3.2608	3 rd	High
Ethics training for employees.	109	2.8372	4 th	Average
Regular key fraud indicator assessments.	109	2.6732	5 th	Average
Whistleblowing policy.	109	2.2839	6 th	Low
Workplace intelligence gathering.	109	1.6521	7 th	Very Low
Forensic background investigation.	109	1.4129	8 th	Very Low
Valid N (list-wise)	109			

Source: Field Survey (2022)

From the Table 1, the three most frequently applied anti-fraud strategies by the business owners are: internal control mechanism, established fraud policies, and good reward system for the employees; in order of their implementations respectively. Inversely, the three least used anti-fraud strategies are whistleblowing policy, workplace intelligence gathering, and forensic background investigation on employees in descending order of their popularities. The business owners (respondents) strongly believe that strong system of internal controls is the most effective antifraud measured by a wide margin, followed by regular fraud risk assessments. This confirms CIMA (2009) findings. Forensic background investigation on employees and workplace intelligence gathering were found to be the least implemented measures. On the contrary, Suponcic (2017) concludes that background investigation on employees is a first line of defence in fraud prevention.

Perceived Impact of Workplace Intelligence Gathering and Forensic Background Investigation on Insider Fraud Threats

Tables 2 and 3 report the responses to the impact of workplace intelligence gathering technique and forensic background investigation on insider fraud threats amongst low-level supply chain business in Nigeria. Further to the Likert five-point scale adopted, ranging from strongly agree to strongly disagree; the respondents were required to rate the perceived capability of workplace intelligence gathering and forensic background investigation on employees in addressing insider fraud threats. Following the guidelines provided by Ho (2006) on data analysis coding; 'strongly agree' was assigned 5 points; 'agree' was assigned 4 points; 'undecided' was assigned 3 points; 'disagreed' was assigned 2 points; and 'strongly disagreed' was assigned 1 point.

Workplace Intelligence Gathering and Insider Fraud Threats

The outcome of the perceived impact of workplace intelligence gathering on insider fraud threats is as reported in Table 2:

Table 2: Perceived Impact of Workplace Intelligence Gathering on Insider Fraud Threats

Scale	No. of Respondents	Percent	Cum. Percent	Mean	S.D	Skew
Strongly Agree	61	55.96	55.96	1.7835	1.125	1.729
Agree	32	29.36	85.32			
Undecided	8	7.34	92.66			
Disagree	6	5.50	98.16			
Strongly Disagree	2	1.84	100.0			
Total	109	100.0				

Source: Field Survey (2022)

From Table 2, approximately 86% of the respondents are of the opinion that workplace intelligence gathering is an effective strategy to counter employee fraud threats; while about 7% disagree with the notion. By implication, there is a positive significant relationship between workplace intelligence gathering on employees and insider fraud threats as showed by the mean score of 1.7835 and standard deviation of 1.051.

Forensic Background Investigation and Insider Fraud Threats

Table 3 reports on the result of the perceived impact of forensic background investigation on insider fraud threats:

Table 3: Perceived Impact of Forensic Background Investigation on Insider Fraud Threats

Scale	No. of Respondents	Percent	Cum. Percent	Mean	S.D	Skew
Strongly Agree	62	56.88	56.88	1.6851	1.162	1.694
Agree	37	33.95	90.83			
Undecided	2	1.83	92.66			
Disagree	5	4.59	97.55			
Strongly Disagree	3	2.75	100.0			
Total	109	100.0				

Source: Field Survey (2022)

In Table 3, nearly 91% of the respondents (sole business owners) are of the view that forensic background investigation on employees is an active measure against workplace fraud threats; while about 7% disagree with the notion. Thus, there is a positive significant relationship between forensic background investigation on employee and insider fraud threats as reveals by the mean score of 1.6851 and standard deviation of 1.162. There is closeness between the results of both Tables 2 and 3.

Table I shows the result of implementation of the eight (8) commonest anti-fraud strategies by the respective business owners. Tables 2 and 3 reported on the effectiveness of both workplace intelligence gathering and forensic background investigation on employees as part of their anti-fraud measures. Table 1 ranking shows that both workplace intelligence gathering and forensic background investigation are hardly incorporated by the business owners. However, Tables 2 and 3 show that the respondents hold the opinions that both strategies are effective anti-fraud strategies. Further, the outcome of the one-on-one online oral interviews conducted with the respondents reveal that the two strategies are least implemented because the process would be costly and weighty giving the financial standing of their firms. Consequently, this paper formulated two hypotheses to determine the level of significant relationship between the two anti-fraud strategies (forensic background investigation on employees and workplace intelligence gathering) (on one hand), and insider fraud threats (on the other hand).

Hypotheses Testing

Two hypotheses were tested to determine the extent of the relationship between workplace intelligence gathering and forensic background investigation on employees (as independent variables), and insider fraud threats (as a dependent variable).

In order to test the hypothesis which states that there is no significant relationship between forensic intelligence gathering technique on employees and insider fraud threats amongst low-level supply chain business in Nigeria, correlation analysis was carried out and the results presented in Table 4.

Table 4: Result of Correlation Analysis

	Intelligence Gathering	Fraud Threats
Pearson Correlation	1	.904**
Intelligence Gathering. Sig. (2-tailed)		.000
N	109	109
Pearson Correlation	.904**	1
Fraud Threats Sig. (2-tailed)	.000	
N	109	109

** Correlation is significant at the 0.01 level (2-tailed).

p-value = 0.000 (< 0.01)

From Table 4, 0.904** (Pearson Correlation Coefficient) reveals a strong positive relationship between workplace intelligence gathering and insider fraud threats. By interpretation, the study could not retain the hypothesis as postulated. As a result, it could be inferred that the higher the level of workplace intelligence gathering on employees, the less the insider fraud threats in the low-level supply chain firms.

In an attempt to test the hypothesis which states that there here is no significant relationship between forensic background investigation on employees and insider fraud threats amongst low-level supply chain business in Nigeria, Correlation Analysis was carried out and the results presented in Table 5.

Table 5: Result of Correlation Analysis

	Background Investigation	Fraud Threats
Pearson Correlation	1	.894**
Background Investigation. Sig. (2-tailed)		.000
N	109	109
Pearson Correlation	.894**	1
Fraud Threats. Sig. (2-tailed)	.000	
N	109	109

** Correlation is significant at the 0.01 level (2-tailed).

p-value = 0.000 (< 0.01)

From Table 5, 0.894** (Pearson Correlation Coefficient) reveals a strong positive relationship between forensic background investigation on employees and insider fraud threats. By implication, the study could not accept the hypothesis two as stated. Hence, it could be interpreted that the higher the level of forensic background investigation on employees, the less the insider fraud threats rate in a given organisation.

Findings from One-On-One Interview Conducted

The outcome of the one-on-one interview conducted among the sole-business owners used for this study reveals as follows: Most firms rarely conduct background investigations on their employees to mitigate on-the-fraud. The level of intelligence gathering strategy among the business owners is significantly low due to feeble level of awareness of the strategy. Slack employment policies, misplaced trust, and fragmented internal control systems create avenues for employees to commit frauds. In Nigeria, there are observed weak legal restrictions on how the low-level business owners process the information collected from background investigations. Employers of labour often outsource background investigation process to agencies, thereby disclosing confidential information about the would-be employee to a third party. If the sensitive information is not properly handled, the approach could have negative consequences on the employee in future.

5. CONCLUSION

This paper explored the relationship between forensic background investigation on employees and insider fraud threats in the low-level supply chain businesses in Nigeria. Employee financial fraud is a type of crime that does not require violence to commit. Completely eliminating on-the-job fraud is practically impossible. Insider fraud threats could ruin a business if left unchecked. Small businesses have an important role to play in the development or growth of every economy. Arguably, in spite of improvements in fraud detection, investigation, resolution and control technologies, financial fraud losses continue to pose a serious problem to many low-level businesses. If instances of these insider frauds are left unaddressed, they would continue to threaten the sustainability of the small-size businesses in Nigeria. The existing traditional anti-fraud techniques have become largely inadequate due to advancements in technology; which inadvertently aid employees to commit fraud.

The solution to the employee fraud lies in adopting forensic background investigation and tactical intelligence gathering approach on employees. It is beneficial for the sole business owners to protect their investments by employing trustworthy individuals; ensure safety of the assets; and holding the reputation of the enterprise. The approach is an evidence-based vital to prevention, detection, investigation and treatment of insider fraud threats. In-house tactical surveillance and

intelligence gathering on employees is a method to build up a detailed knowledge of threats to an organisation. The assessment and forensic investigation process help make decisions about how to respond to these threats and what protective measures to take. Pre-employment and on-the-job forensic background investigation and tactical intelligence gathering on the employees should be part of the standard anti-fraud strategy of the firm. Credibility in the information gathered and intelligence report generated on the employees must be a hallmark. An employer seeking to engage a third-party professional to carry out background investigations on its behalf is expected to carry out the appropriate level of due diligence to ensure that the professional firm is capable of complying with all obligations.

References

- Adu, D. (2018). Nigeria: Background checks on employees: Retrieved from <http://www.mondaq.com/Nigeria>.
- Akuh, C. G. (2017). Small retail business strategies to detect and prevent employee fraud. *Walden Dissertations and Doctoral Studies*, Walden: Walden University.
- Albrecht, W. S. (2014). Iconic fraud triangle endures: *July/August Fraud Magazine*. New York: Association of Certified Fraud Examiners (ACFE).
- Albrecht, W. S., Romney, M. B., Cherrington, D. J., Payne, I. R. & Roe, A. V. (1982). *How to detect and prevent business fraud*. Cliffs, NJ: Prentice Hall Prentice-Hall.
- Bichanga, S. (2019). *9 steps of forensic investigation*. Delaware: International Institute of Certified Forensic Investigation professionals (IICFIP).
- Blanchard, D. (2010). *Supply chain management best practices*, (2nd ed.). New York: John Wiley & Sons.
- Bohan, T. L. (2010). Strengthening forensic science: A way station on the journey to justice. *Journal of Forensic Science*, 5(3), 5-7.
- Chatman, Q. (2009). *How scientific is forensic science?* Retrieved from <http://www.nacdl.org/public.nsf>
- Coenen, T. L. (2009). *Expert fraud investigation: A step-by-step guide*. New Jersey: John Wiley & Sons.
- Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. New York: The Free Press.
- Creswell, J. W. (2008). *Educational research: Planning, conducting and evaluating quantitative and qualitative research*, (3rd ed.). Cupane: Pearson Prentice Hall.
- Dutta, S. K. (2013). *Statistical techniques for forensic accounting understanding the theory and application of data analysis*. New Jersey: Pearson Education.
- Ho, R. (2006). *Handbook of univariate and multivariate data analysis and interpretation with SPSS*. Boca Raton: Chapman & Hall.
- Homer, E. M. (2019). Testing the fraud triangle: A systematic review. *Journal of Financial Crime*, 27(1), 172-187.
- Ignou, N. K. D. (2012). Selection of the research paradigm and methodology. *Online Research Methods Resource for Teachers and Trainers*, 2(1).
- Langner, D. (2010). Employee theft: determinants of motive and proactive solutions. UNLV *Theses, Dissertations, Professional Papers, and Capstones*. 543.

- Levashina, J. & Campion, A. (2009). Expected practices in background checking: Review of the human resource management Literature. *Employee Responsibilities and Rights Journal*, 21, 231–249.
- Lucas, S. R. (2014). An inconvenient dataset: Bias and inappropriate inference in the multilevel model. *Quality & Quantity*, 48, 1619-1649.
- Marks, J. (2012). The mind behind the fraudsters crime: Key behavioral and environmental elements. In ACFE Global Fraud Conference. Association of Certified Fraud Examiners.
- Okaro, S. C. & Okafor, G. O. (2013). Drivers of audit failure in Nigeria: Evidence from Cadbury (Nigeria) PLC. *Research Journal of Finance and Accounting*, 4(6), 1686-1697.
- Omar, M., Nawawi, A. & Puteh, A. S. A. (2016). The causes, impact and prevention of employee fraud: A case study of an automotive company. *Journal of Financial Crime*, 23(4), 1012-1027.
- PBL Blackwell (2010). *Forensic psychology*. Towl & Crighton (ed.), West Sussex: The British Psychological Society and Blackwell.
- Peprah, W. K. (2018). Predictive relationships among the elements of the fraud diamond theory: The perspective of accountants. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 8(3), 141–148
- Ramamoorti, S., Morrison III, D. E., Koletar, J. W. & Pope, K. R. (2015). A.B.C.'s of behavioral forensics: Applying psychology to financial fraud prevention and detection. New Jersey: John Wiley & Sons.
- Ruankaew, T. (2016). Beyond the fraud diamond. *International Journal of Business Management and Economic Research*, 7(1), 474-476
- Said, J., Alam, M.M., Ramli, M., & Rafidi, M. (2017). Integrating ethical values into fraud triangle theory in assessing employee fraud: Evidence from the Malaysian banking industry. *Journal of International Studies*, 10(2), 170-184.
- Small, L. (2015). 4 risks your company takes when background checks are not a part of your hiring process. Retrieved from <https://www.greenhouse.io/blog>.
- Suponcic, F. (2017). Background checks: the first line of defense in fraud prevention. Retrieved from <https://skodaminotti.com/blog/background-checks-first-line-defense>.
- Sutherland, E. H. (1939). *Principles of criminology*. Chicago: J.B. Lippincott
- The Association of Certified Fraud Examiners (ACFE) (2018). *Fraud examiners manual*. (International ed.), Austin: ACFE.
- The Chartered Institute of Management Accountants (CIMA) (2009). *Fraud risk management: A guide to good practice*. (CIMA Technical Guide), London: CIMA.
- The International Academy of Forensics (IAF) (2019). *Forensic investigation and criminal intelligence narratives*. IAF: Lagos.
- The National Research Council (2000). *Surviving supply chain integration: Strategies for small manufacturers*. Washington, DC: The National Academies Press.
- Wolfe, D. T. & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, December, 1-5.
- Yekini, K., Ohalehi, P., Oguchi, I. & Abiola, J. (2018). Workplace fraud and theft in SMEs: Evidence from the mobile telephone sector in Nigeria. *Journal of Financial Crime*, 25(4), 969-983
- Zuberi, O. & Mzenzi, S. I. (2019). Analysis of employee and management fraud in Tanzania. *Journal of Financial Crime*, 26(2), 412-431.