Journal of Social Economics Research
2019 Vol. 6, No. 2, pp. 188-201
ISSN(e): 2312-6264
ISSN(p): 2312-6329
DOI: 10.18488/journal.35.2019.62.188.201

WHAT ARE THE CONTEXTUAL INFLUENCES OF BANK CRIMINALITY IN OSUN EAST SENATORIAL DISTRICT?

Taofik, Olatunji Bankole

Department of Demography and Social Statistics, Faculty of Social Sciences, Obafemi Awolowo University, Ile-Ife, Nigeria.

Article History
Received: 13 September 2019
Revised: 16 October 2019
Accepted: 26 November 2019
Published: 2 January 2020

Keywords
Bank criminality
Human induced factors
Security mechanism
Contextual influences.

ABSTRACT

The threats posed by bank criminality to nation building are such that an emerging nation such as Nigeria must not overlook. In spite of its negative implications, previous studies addressing the menace have either adopted the descriptive approach or focused majorly on reoccurrence of armed robbery during the festive periods. Also, there is a dearth of studies that employed the mix-methods approach and adopted the tripartite analysis technique to examine the causal effect association between bank criminality and its predictors. This study addresses these limitations by asking this question; what are the contextual influences of the various forms of bank criminality in Osun East Senatorial District? The outcome variable of the study was bank criminality, and the explanatory variables were contextual influences and broadly categorised into security mechanisms and human induced factors. Stata version 14 was employed in quantitative data analysis while the qualitative data was analysed using content analysis. Results showed that security mechanisms (χ^2=17.502; p<0.001; χ^2=8.467; p<0.037; χ^2=11.09; p<0.004; χ^2=7.876; p<0.049; χ^2=16.233 p<0.001; χ^2=10.954; p<0.01) and human induced factors(ß = -0.226; t= -4.44; p<0.000; ß = 0.173; t=2.52; p<0.015; ß = 0.147; t=3.87; p<0.007; ß = -0.136; t= -2.56; p<0.013; ß = -0.206; t= -3.53; p<0.001) were predictors of bank criminality The study conclude that bank human induced factors, that is, bank employees' efficiency and security mechanism functionality are indispensable to curtailing various forms of bank criminalities.

Contribution/Originality: This study contributes in the existing literature by investigating the contextual predictors of bank criminality beyond the conventional approach; it documents the influences of human induced factors and security mechanisms on bank criminality, as such document provides insights to preventing banks and their customers from losing funds and vital information to criminals.

1. INTRODUCTION

In Nigeria, the incidence of crime, especially as it relates to cyber and internet banking scam is no doubt on the rise over the past few decades. Retrospectively, bank criminality in Osun East senatorial district is no exception. In fact, across financial institutions in Nigeria, bank criminality remains one of the major challenges faced by financial institutions in service delivery to their customers (Hassan *et al.*, 2012). The incidence of criminality in many of the banks across communities in Nigerian has been a prime concern. As a matter of urgency, the danger posed by bank criminality cannot be over-looked. This is needful, when especially the persistent incessant of internet fraud,

impersonation and reported cases armed robbery attacks across communities is taken into consideration (Ebele, 2012).

Imperatively, criminality in many financial institutions, particularly amongst operators of commercial banking in the country has in no doubt transpired from impersonation, internal and external fraud to e-theft, automated teller machine fraud. A few studies have allied the vulnerability account holders to criminals to poor handling, as well as non-functionality of modern information technologies that many commercial banks in the country now use (Olumide and Balogun, 2010; Parthiban and Raghavan, 2014). In fact, with the incipient cases of impersonation, internal and external fraud, among the likes, the incidence of criminality in the country calls for re-strategized bank security (Wada and Odulaja, 2012).

Empirically, the inability of many banks in the country to adequately address rise in security lapses in many of their bank branches remains a critical issue, and this calls for immediate attention (Salawu, 2010; Federal Bureau of Investigation, 2016). As a result, the endemic challenges resulted from unparalleled victimization of banks in the country; and this was pertinent not just from the internal but also external sources (Aremu and Ahmed, 2011). As identified by Stone (2011) there is no doubt that the continuous improvements in the information technology have significantly obstructed banking operations and services across regions of the world; and Nigeria banks are no exception.

Thus, there is no doubt that practically all financial institutions to a very large extent depend on information technology facilities in the delivery of financial services such as e-money, e-brokering, e-insurance, e-finance, e-exchange and not limited to e-banking to their customers or clients as the case may be (Adams, 2010; Ebele, 2012). For instance, e-banking, particularly the provision of the automated teller machines is a huge innovation in the banking sector that has brought about quicker service delivery to bank customers. In fact, Michael *et al.* (2014) and Ebele (2012) maintained that banking product and services were more effective and faster these days between banks and their customers via electronic interactive communication channels than it used to be in a about two decades back.

As a result of the inexorable consequences of bank criminalities to nation building, several studies have attempted to examine the phenomenon. However, a high proportion of previous studies on the subject matters have focused majorly on armed robbery (Olumide and Balogun, 2010; Moses-Òkè, 2012; Wada and Odulaja, 2012). It was also noted that previous studies that have examined bank criminalities in the country had concentrated on analysis the menace from the descriptive view (Daniel, 2006; Otu, 2010; Hassan *et al.*, 2012; Okeshola and Adeta, 2013; FBI, 2016). In fact, there is a dearth of studies that have adopted simultaneously employed both the qualitative and quantitative method is explaining the predictors of bank criminality in the country. These observed gap in literature prompted the need for this study. This study addresses these limitations by asking this question: what are the contextual influences of the various forms of bank criminality? Hence, the broad objective of this study was to explore the contextual predictors of bank in Osun East Senatorial District of Osun State Southwest, Nigeria.

1.1. Literature Review

There are no innovations without one or two negative implications. Invariably, banking innovation is no exception. For instance, banking innovation in the country was argued by Olumide and Balogun (2010) to have brought about rise in the incidence of e-theft. These criminal activities ranges from data theft, card cloning to transpire unauthorised entering into and bank and customer accounts by hackers. The negative implications of e-banking criminality are not farfetched. In fact, the advent of e-banking services poses a big threat to bank customers, personal data and capitals. As noted by Okeshola and Adeta (2013) the introduction of e-banking in Nigeria has provide bank fraudsters with more breaks to divert funds from genuine bank customers who are in most cases not physically present on the web to authenticate the illicit financial transaction. Retrospectively, several unauthorised access of legitimate bank customers by hackers have resulted in huge loss of capital of confidential

data. Therefore, it could be deduced these findings (Okeshola and Adeta, 2013) that e-banking services have brought about new kinds of criminality on the e-platform, which vary from pin theft to automated teller machine card cloning.

As noted by Michael *et al.* (2014) the sequence of bank insecurity as it relates to fund safety, data protection arising from unauthorised hacking of bank sensitive depositories through breaking of codified files, fears are now being created in the minds of bank customers in Nigeria. The situation has worsen to the extent that legitimate customer is safe, since no one knows who is going to be the next victim (Michael *et al.*, 2014). In fact, the status quo was so dismal that bank criminalities have led to alternating bank closures against customers' desire, and this has upsurge the risk of working in the banking sector (Moses-Òkè, 2012).

According to Moses-Òkè (2012) financial dealings were considered as such which come with severe risks. In fact, people have resulted to avoiding passing through where banks are situated for fear of being caught unaware due to incessant of bank armed robbery (Shah, 2012). Similarly, Maitanmi *et al.* (2013) noted that sometimes, bank criminalities, especially such the unauthorised of funds had been attributed to cooperation with some staff within the banks and at times, retrenched or sacked staff.

Comparatively, in the recent time, studies (Ebele, 2012; Hassan *et al.*, 2012; Wada and Odulaja, 2012; Michael *et al.*, 2014; Ndible, 2016) have identified some forms of reoccurring bank criminalities, and these include: automated teller machine pin theft, automated teller machine cloning, internet banking fraud, and the likes. As noted by Salawu (2010) the incessant incidence of brank criminalities had brought about an intense rise to demanding use of digital security features. according to Michael *et al.* (2014) the passive involvement of the government of Nigeria in state security, which was quite inconsequential had placed an enormous obligation on bank operators to invest heavily in the procurement of advanced security mechanisms in order to safeguard the huge capital and vital information entrusted in their care.

Thus, the predominant and incessant incidence of bank criminalities in Nigeria calls for stern approach and accentuates the necessity for banks to balance their business operations with safety. As argued by Maitanmi *et al.* (2013) and Aremu and Ahmed (2011) there is an urgent need for safety in bank operations in Nigeria, given the fact that county is a predominately cash-based economy. For instance, apart from the monetary implications of bank robberies, the distress and moral frights that armed robbers are likely to engender may have a much more deleterious consequence in the community as a whole (Ebele, 2012; Roberts, 2013). Imperatively,, there is need to correct the state of affairs, taking into consideration the roles of banks in the socio-economic development of a nation.

Ndible (2016) observed that the adoption of bank security mechanism in banking business has not only revolutionized but also re-defined the methods banks are now operating in the country. He attributed these developments in the financial sector to the fact that there was a need to curtail the degree of crime in the business world (Ndible, 2016). It could then be deduced from these arguments that the kinds of security mechanisms adopted by banks will either hamper or boost its operations and service delivery at large. In the case of post-robbery investigation, security mechanisms have equally helped police in their findings (Ebele, 2012). More so, bank security incorporates a number of levels and components, which include physical security mechanisms - vault, lockers, boxes, security guards, police – as well as digital security – automated teller machine, surveillance cameras, audio system, alarm systems, closed circuit television, monitors and many more (Wada and Odulaja, 2012; FBI, 2016).

There is no doubt that banks now installed these sophisticated security mechanisms in their branches, this is with the view to averting fraud, identifying on-going and concluded fraud, protecting customers' assets and promoting returns on investment (Michael *et al.*, 2014). This is inevitable since security in banks is indispensable to profitability and safe banking environment (Alex, 2010; Smith, 2012). It was noted by Aremu and Ahmed (2011) that form of security devices required by banks in the country was influenced by types of transaction banks operate.

Nearly all banks in Nigeria were under-secured while a very few were over-secured; thus, a high number of banks in the country was helpless to bank determines criminality (Hassan *et al*., 2012). According to Parthiban and Raghavan (2014) bank criminalities could lead to indecisive consequences, while poor security could condense high exposure to criminality, thereby uncovering the facility to criminality.

In the meantime, effective handling of accessible security mechanism could define the extent of vulnerability to bank criminalities (Moses-Òkè, 2012). In spite of the significant rise in bank criminalities in Nigeria, substantive measures are yet to be taken in view to tackling the act successfully.

1.2. Theoretical Focus: Routine Activity Theory (Cohen and Felson, 1979)

This study is underpinned by the Routine Activity Theory propounded by Cohen and Felson (1979). The Routine Activity Theory posits that for crime to ensue, three basics are inevitable. First, an individual must be motivated to initiate the crime; two, there must be a vulnerable victim and three, there must an insufficient protection to avert such impending crime. The routine activity theory provides an unpretentious and potent insight into the causes of crime evils. According to the proponents of the theory, it was assumed that crime will only take place where the individual offender is enthused by interest or by ability to weigh the means and aims where handlers or cub able guardians' are absent, weak or corrupt and targets, or victims. As assumed by Cohen and Felson (1979) all things being equal, criminality is a function of the convergence of three factors in time and space. Imperatively, the routine activity theory gives an explicit and detailed explanation for a plausible relationship between bank criminalities, human induced factors and security mechanisms available at banks.

This theory recognises the psychology of crime as it elucidates that without a target and individual or group cannot commit a crime in the emptiness which any money bank in Nigeria is a seemly target of any enthused offender who is prepared to take the risk to acquire what belongs to someone else by evaluation of the risk and the gain putting into consideration the available guardian weakness. Thus, the availability of cash within a bank and weak security to protect it against hacker, armed robber or fraudster who is enthused to commit a successful crime may take place. Similarly enthused employee of a bank willing to commit fraud already present in the target zone and recognises the weakness of culpable guardians available will perpetrate the crime successfully. Hence, the routine activity theory is found appropriate for this study.

2. METHODS

2.1. Data Source and Research Design and Data Source

The study was a cross-sectional survey and it employed the retrospective research approach. The retrospective design was considered appropriate since the study was limited to sourced information within the span of 2012 to 2017. Also, this is with the view to providing an insight in the trends of forms of criminality as well as the extent of susceptibility of the purposely selected bank branches covered in the study. The cross-sectional design was justifiable since information was sourced at a point in time with the view to addressing the stated broad objective of the study. Primary and secondary data was sourced for this study from the professional staff, teller officers and security personnel from the selected bank employees between the aforementioned time span.

2.2. Sampling Technique and Sample Size

The purposive and snowball sampling technique was adopted in this study. The inclusive criteria for the selection of banks for the study were based on the availability of branches of the selected bank in the studied area within the study period time frame (2012 to 2017). Therefore, only bank employees with at least five years working experience in the banking operation were included considered legible and included in the selected study locations. The snowball approach was adopted where there were more legible bank employees than the targeted respondents in such bank branch. The study focused on eight (8) purposely selected banks comprising both new and old

generation banks. The selected banks are First Bank, Union Bank, Polaris Bank (formerly Skye Bank), Guarantee Trust Bank, Access Bank, Zenith Bank, Eco Bank and United Bank for Africa respectively. The two purposively selected communities were Ile-Ife and Ilesa town. One bank branch was selected each in each of the eight (8) selected banks across the two purposefully selected communities. One professional staff, one teller and one security were covered in each of the covered banks. Three (3) bank employees were captured in each of eighteen banks across in the two (2) covered communities. Therefore, a total sample size of forty-eight (48) bank employees was captured in the study.

2.3. Research Variables and Research Instrument

The outcome variable was bank criminality and it was captured in form of e-banking fraud, cheque fraud, theft and impersonation. The explanatory variables of the study were preventive mechanisms and human induced factors respectively.

2.4. Data Analysis

The sourced primary data were entered directly into SPSS (SPSS version 25 for Windows, SPSS Inc., Chicago IL). The gathered data were sorted, cleaned and further exported to Stata version 14. All statistical analyses were carried out with the Stata version 14. Using the appropriate descriptive statistics, the different forms of bank criminalities were presented in tables and percentages. The chi-square test was carried out at the second level of analysis to establish the relationship between bank criminality and contextual influences. The linear regression was employed at the third level of analysis. The multivariable linear regression was carried out to establish the causal-effect association between the bank criminality (outcome variable) and explanatory (preventive mechanisms and human induced factors) variables of the study.

3. RESULTS

3.1. Distribution of Respondents by Various Forms of Bank Criminalities

Results of the study by forms of bank criminalities as presented in Table 1 showed that about two-thirds (64.6%) of the respondents stated that they received cases of internet frauds in their banks. Also, the results showed that three (60.45) in every five of the respondents admitted that they received reported cases of cheque frauds in their banks. 45.8% of the respondents reported that one form or another of bank criminalities was reported in the last 11 months or less in their bank branches. More than three-quarters (87.5%) of the respondents stated that they received cases of ATM frauds in their bank branches. contrarily, results by bank theft showed that less than one-third (29.2%) of the respondents maintained that they had cases of bank theft in their bank branches. About 70% of the respondents linked sources of the last bank criminalities at their bank branches to internal sources while one-third (33.3%) of the respondents admitted to receiving reported cases of impersonation in their bank branches.

The analysis below-mentioned was compiled from the findings of in-depth interviews conducted with the bank employees whose identities were captured numerically and on fictitious names based on no specific order for confidentiality sake as follows:

> A Customer at our branch collected his Debit card…and was activated by the same customer on the ATM inside the Ilesa branch premises ATM. Two days after, the customer came to withdraw from our branch ATM and called on another customer to assist him with how to use the ATM. The customer inserted the card into the ATM with the pretense that he wanted to assist, but only to be informed that his ATM was not dispensing cash. Upon getting to another bank ATM, it was discovered that the ATM had been charged. A few minutes after, transactions alert were being received by him and before the

account was blocked, the fraudster had already withdrawn a sum of One Hundred Thousand naira (₦100,000.00) only from the account (A Bank Crime Incidence Reported by a Male Professional Employee, 2019).

Table-1. Distribution of respondents by forms of bank criminalities.

Forms of Bank Criminalities	Prevalence of Bank Criminalities	
	n = 48	(%)
Incidence of any Form Bank Criminalities		
<12 months	22	45.8
1-4 years	15	31.3
5 years or more	11	22.9
Reported cases of Internet Fraud		
Yes	31	64.6
No	17	35.4
Reported cases of cheque fraud		
Yes	29	60.4
No	27	39.6
Reported cases of ATM fraud		
Yes	42	87.5
No	6	12-5
Reported cases of bank theft		
Yes	14	29.2
No	34	70.8
Reported cases of Impersonation		
Yes	16	33.3
No	32	66.7
Linked sources to last bank criminalities at this branch		
External	3	6,3
Internal	35	72.9
External/Internal	10	20.8

Source: Field survey, 2019.

I received a phone call from the security guards in one of our bank branches informing me of robbery on our Bank ATM and other banks ATMs…the vault doors were removed with an oxy-acetylene flame. A total of Two Million Seven Hundred and Fifty Two Thousand Five Hundred naira only (₦2,752,500.00) was taken from the ATM (A Bank Crime Incidence Reported by a Male Southwest Regional Manager, 2019).

A bank customer walked into the bank branch to make a cheque withdrawal of Two Million Five Hundred and Eighty-Two Thousand (₦2,582,000.00) naira only on a third party account .Cheque was verified and was sent for confirmation from the domicile branch. The account officer confirmed the payment and customer was paid using his driver's license. After about 50 minutes the account holder visited of the domicile branch to complain of a withdrawal on his account. It was discovered that the withdrawal was fraudulent…all effort to reach the phone number provided by the fraudster proved abortive ([A Bank Crime Incidence Reported by a Male Branch Control Manager, 2019).

3.2. Distribution of Respondents by Human Induced Factors and Bank Security Mechanisms

Results by human induced factors and bank security mechanisms as presented in Table 2 showed more than half of the respondents were of the view that external e-banking crimes were often linked some customers of the bank while about three-quarters of the respondents disagreed that some cases of e-banking frauds had been linked to some customers of the bank. Relatively, at least four (81.2%) in every five respondents disagreed that security recording devices were backed-up outside the bank branch while a significant amount (85.4%) of the respondents were of the opinion that security devices functionality could not be altered without adequate approval. Likewise, the outcomes of the study showed that almost all (95.8%) the respondents agreed that security mechanism in their bank branches were not accessible by unauthorised individuals.

Table-2. Distribution of respondents by human induced factors and bank security mechanisms.

Variables	Influence of Human Induced Factors	
	n = 48	(%)
External e-banking crimes are often linked to some customers of the bank		
Agreed	28	58.3
Disagreed	20	41.7
Some e-banking frauds committed have been linked to some customers of the bank		
Agreed	11	22.9
Disagreed	37	77.1
Security recording devices are backed-up outside the bank branch		
Agreed	9	18.8
Disagreed	39	81.2
Security devices functionality cannot be altered without adequate approval		
Agreed	41	85.4
Disagreed	7	14.6
Security mechanism in your branch is not accessible by unauthorized persons		
Agreed	46	95.8
Disagreed	2	4.2

Source: Field survey, 2019.

3.3. Distribution of Respondents by Type of Security Mechanisms Used in Prevention of Bank Criminalities at their Various Bank Branches

Results of the study by security mechanisms used in prevention of bank criminalities as presented in Table 3 showed that all (100.0%) the respondents reported that ATM cameras, private security, CCTV/DVR, Man trap doors, Burglary proofs, police officers and vault-proof doors were put in place in their bank branches with the view to averting and tackling bank criminalities. On the other hand, less than half (43.8%) admitted that there were in surveillance cameras in their various bank branches to prevent bank criminalities. Nearly all the respondents (97.9%) reported that alarm systems were readily available in their various bank branches as required to prevent criminalities in banks. The results further showed that majority (91.7%) of the respondents reported that their bank branches PC and system security while about two-thirds (68.8%) admitted that pepper-sprays were readily available in their bank branches. Likewise, the results showed that majority (93.8%) of the respondents reported that there were safe-deposit boxes in their bank branches. equally, about 96% of the respondents reported that fire alarm were readily available in their bank branches.

Table-3. Distribution of respondents by security mechanisms used in crime prevention.

Variables	Functionality of Security Mechanism	
	n = 48	(%)
ATM cameras		
Yes	48	100.0
No	0	0.0
Surveillance cameras		
Yes	21	43.8
No	27	56.2
Private security		
Yes	48	100.0
No	0	0
Alarm systems		
Yes	47	97.9
No	1	2.3
CCTV/DVR		
Yes	48	100.0
No	0	0.0
PC/system security		
Yes	44	91.7
No	4	8.3
Man-trap doors		
Yes	48	100.0
No	0	0.0
Burglary proofs		
Yes	48	100.0
No	0	0.0
Pepper-sprays		
Yes	33	68.8
No	15	31.2
Police officers		
Yes	48	100.0
No	0	0.0
Safe-deposit boxes		
Yes	45	93.8
No	3	6.2
Vault-proof doors		
Yes	48	100.0
No	0	0.0
Fire alarm		
Yes	46	95.8
No	2	4.2

Source: Field survey, 2019.

The analysis above-mentioned was compiled from the findings of in-depth interviews conducted with the bank employees whose identities were captured numerically and on fictitious names based on no specific order for confidentiality sake as follows:

> There was a successful attack against Polaris bank. Oxy-acetylene flame was used to bring down the vault door of the bank and millions of naira taken away from the ATM. The security men attached to the ATMs together with nearby institution security guards were enclosed and tied with tick rope; however, the invasion on Guarantee Trust Bank was unsuccessful with their installed pepper spray (A Bank Robbery Incidence Reported by a Male Branch Control Manger, Ilesa, 2019).
>
> Unknown armed robbery gang of about seven men broke into two banks ATM. At about 2:30 AM and successfully made away with over Four million

(₦4,000,000.00) naira…there was an attempt on our GTBank ATM, the iron door was broken and attempt was made to go into the ATM, but the robbers were prevented by the automated activation of the pepper spray in the ATM which discharged 'tear gas' making the ATM room uncomfortable and also with a sound of an alarm which prompted them to leave. All the private security guards were tired and locked down (A Bank Crime Incidence Reported by a Female Customer Service Manager Professional, 2019).

3.4. Distribution of Respondents by Bank Criminalities (e-banking) and Bank Security Mechanisms

The chi-square analysis results presented in Table 4 showed that there is significant relationship between linkages of eternal e-banking to internal sources from the bank and internet banking fraud cases (χ^2 =17.502; p<0.001). The result shows that more than half (54.5%) of the respondents agreed that the occurrence of internet frauds in banks had link with internal source from the bank. Similarly, the results showed that internet banking and backing-up of security recording devices were significantly associated (χ^2 =8.467; p<0.037). The results further showed that the result showed two in every five (40.0%) of the respondents agreed that internet banking frauds would have been prevented if their branches had backed up devices outside their branches. Our results equally showed that altering of security devices without adequate approval from management and internet banking fraud were significantly associated (χ^2 =11.09; p<0.004).

Furthermore, the study showed that more than half (56.5%) of the respondents agreed that incidence of internet banking frauds would not have been averted in their bank branches if the security mechanisms had not been altered by unauthorized persons. Similarly, the outcomes of the study showed Cheque frauds and e-banking transactions by initiated by some bank customers were significantly associated (χ^2 =7.876; p<0.049). Relatively, ATM fraud bank was found to be significantly associated with banking up of banking security mechanisms outside the bank branch (χ^2 =16.233 p<0.001). The results further showed that more than three-quarters (80.0%) of the respondents admitted that ATM frauds would have been averted if their bank branch were not backed up outside their bank branches. Impersonation (money transfer) and linking of external e-banking crimes to internal source from internal source from the bank were found to be significantly associated (χ^2 =10.954; p<0.012).

On the other hand, nearly (92.7%) the respondents did not accept that impersonation in banks had links with internal source from the bank. Also, the result also showed that there was a strong significant relationship between altering of security devices without adequate approval from management and Impersonation (χ^2 =14.803; p<0.01).

Therefore, the outcomes of our study at the bivariate level of analysis showed that bank criminality are significantly influenced by security mechanisms across the selected banks in Ile-Ife and Ilesa communities in Osun East Senatorial district, Osun State, Southwest Nigeria.

Table-4. Chi-square results showing relationship between bank criminalities (e-banking) and bank security mechanism.

Variables	Internet banking fraud cases were recorded at this branch		
	Yes (%)	**No (%)**	**p-value**
External e-banking crimes were linked to internal source from the bank			
Disagreed	6.7	93.3	0.001**
Agreed	54.5	45.5	
χ^2; df	17.502; 3		
Variables	Internet banking frauds cases were recorded at this branch		
	Yes (%)	No (%)	p-value
Security recording devices are backed up outside the bank branch			
Disagreed	41.5	58.5	0.037*
Agreed	40.0	60.0	
χ^2; df	8.467; 3		
Variables	Internet banking fraud cases were recorded		
	Yes (%)	No (%)	p-value
Security devices functionality cannot be altered without adequate approval			
Disagreed	56.5	43.5	*0.004***
Agreed	26.3	70.7	
χ^2; df	11.09; 2		
Variables	Cheque fraud cases were recorded at this branch		
	Yes (%)	No (%)	p-value
Some e-banking frauds committed have been linked to some customers of the bank			
Disagreed	0.0	100.0	*0.049**
Agreed	43.9	56.1	
χ^2; df	7.876; 3		
Variables	ATM frauds were recorded at this branch		
	Yes (%)	No (%)	p-value
Security recording devices are backed up outside the bank branch			
Disagreed	92.7	7.3	*0.001***
Agreed	80.0	20.0	
χ^2; df	16.233; 3		
Variables	Impersonation (Money Transfer)		
	Yes (%)	No (%)	p-value
External e-banking crimes were linked to internal source from the bank			
Disagreed	6.7	93.3	*0.012**
Agreed	45.5	54.5	
χ^2; df	10.954; 3		
Variables	Impersonation (Money Transfer)		
	Yes (%)	No (%)	p-value
Security devices functionality cannot be altered without adequate approval			
			*0.001***
Disagreed	0.0	100.0	
Agreed	52.2	47.8	
χ^2; df	14.803; 2		

Note: *Significant at p<0.05, **Significant at p<0.01, ***Significant at p<0.001.

3.5. Results of Simple Linear Multivariate Regression Analysis Showing Causal-effect Association between Bank Criminalities and Bank security Mechanisms

As presented in Table 5 the linear multiple regression was employed to analyse the effects of human factors and bank security mechanisms on occurrence of bank criminalities in Ile-Ife Community, Osun State, Nigeria. The results showed that there was internet banking fraud and linking of external e-banking crime to internal source from the bank were inversely and significantly associated (ß = -0.226; t= -4.44; p<0.000). Relatively, the result

showed that the existence of a direct and significant association between internet banking fraud and alteration of bank security mechanism functionality (ß = 0.173; t=2.52; p<0.015). More so, the results similarly established the existence of a positive and significant association between the alteration of banking security mechanisms by unauthorized persons and cheque fraud in bank are not significantly associated (ß = 0.147; t=3.87; p<0.007). Equally, the results of our study further showed that bank theft and linking of external e-banking crime to internal source from the bank were inversely but significantly associated (ß = -0.136; t= -2.56; p<0.013). Correspondingly, there exists a negative but a significant relationship between cheque fraud in bank and linking of external e-banking crime to internal source from the bank are negative (ß = -0.206; t= -3.53; p<0.001). Hence, the outcomes of the multivariate level of analysis in this study showed that human induced factors and bank security mechanism and bank criminalities were significantly associated (P<0.05). Thus, there is a causal-effect association between the response and explanatory variables of this study.

Table-5. Simple linear regression results showing relationship between human factors, bank security mechanisms and bank criminalities.

Human Factors and Bank Security Mechanisms	**Bank criminality (Internet Banking Fraud)**			
	ß	**t-test**	**p-value**	**C.I. (95%)**
External e-banking crime linked to internal sources from the bank	-0.2258	-4.44	0.000***	-0.3276 -0.1240
Security devices functionality cannot be altered without adequate approval	0.1731	2.52	0.015*	0.0354 0.3108
_cons	1.6214	5.92	0.000	1.0728 2.1699
Human Factors and Bank Security Mechanisms	Bank criminality (Cheque Fraud)			
	ß	t-test	p-value	C.I. (95%)
External e-banking crimes are often linked to internal sources from the bank	-0.2059	-3.53	0.001**	-0.3228 -0.0890
Security devices functionality cannot be altered without adequate approval	0.1472	3.87	0.007**	-0.0108 0.3053
_cons	1.4803	4.71	0.000	0.8506 2.1100
Human Factors and Bank Security Mechanisms	Bank criminality (Theft)			
	ß	t-test	p-value	C.I. (95%)
External e-banking crimes are often linked to internal sources from the bank	-0.1356	-2.56	0.013*	-0.2419 -0.2938
Security devices functionality cannot be altered without adequate approval	0.1184	1.65	0.104	-0.0251 0.2621
_cons	1.6627	5.82	0.000	1.0903 2.2350
Human Factors and Bank Security Mechanisms	Bank criminality (Impersonation)			
	ß	t-test	p-value	C.I. (95%)
External e-banking crimes are often linked to internal sources from the bank	-0.1939	-3.66	0.001**	-0.3002 -0.0877
_cons	1.9379	13.06	0.000	1.6409 2.2350

Note: *Significant at p<0.05, **Significant at p<0.01, ***Significant at p<0.001.

3.6. Discussion of Findings

The findings of the study have examined in full the various types of criminalities that have occurred in the selected banks. Correspondingly, the study has been able to identify the numerous security mechanisms that these selected banks used to prevent or detect bank criminalities. Furthermore, the direction relationship between banking criminalities and security mechanisms used against crimes in banks has been determined in course of the study. More so, the human factors in the effectiveness of the existing banking security mechanism were being accessed in this study.

The results of the study showed that bank criminalities were categorized into two. The first being e-banking crimes; which were sub-grouped into: internet banking fraud, cheque frauds, ATM fraud, bank theft and impersonation through money transfer. Gathered facts in this study showed that t ATM frauds was the most committed e-banking crime, while bank theft and impersonation were the least committed crimes via the electronic

platforms provided by these selected banks. These findings conform to that of Ndible (2016); FBI (2016) and Okeshola and Adeta (2013) which identified perpetuation of frauds via the e-banking system as the leading bank criminality.

Also, the study focused on investigating and identifying the various forms of banking security mechanism that were on ground in the study location. ATM camera, CCTV/DVR, Man-trap doors, Vault-proof doors were found to be in presence in all the investigated selected banks. On the other hand, Pepper-sprays were found not to be used at all the selected banks. The results showed that a significant proportion of the respondents admitted that their banks did not have this security device installed at the moment.

Contrarily, virtually all selected banks in this study had Fire alarm Burglary-proofs installed in their banks to protect against external attacks. Other identified security mechanisms in these banks were Safe-deposit boxes and PC/System security which were provided by the virtually all the banks investigated. Comparatively, all the aforementioned security mechanisms across the selected banks were found to be functional. The presence of these security mechanisms were in accordance with the fact that safety of lives and properties in banks were paramount to banks, and this is in line with the argument of Michael *et al.* (2014) and Moses-Òkè (2012) Also, this shows that banks were investing in security safety devices with the main goal of preventing and reducing not only internal crime but also external frauds. In fact, these findings corroborated with Wada and Odulaja (2012); Shah (2012) and Salawu (2010) that affirmed that banks were investing in security mechanisms to prevent both internal and external frauds.

Retrospectively, findings from the study has evidently revealed that bank criminalities in the studied location, which is a representation of the situation of thing across banks in the country. In fact, some reported cases of bank criminalities, especially those that were related to e-banking would have been averted if there had safer security mechanisms. It was evident from this study that some banks in the country were yet to provide functional security mechanisms while there seemed to poor integration of both human and security devices in such a way that bank customers would have been less vulnerable to internet fraudsters.

Thus, findings from this study have empirically established that bank criminality in the studied banks was solitarily influenced by human induced factors nor unilaterally by the extent of security mechanism functionality rather both factors had significant influence on the phenomenon. Hence, the outcomes of this study has revealed that human induced factors and security mechanisms are fundamental contextual predictors of bank criminalities in Osun East Senatorial District.

3.7. Conclusion

The study on bank criminalities in Ile-Ife community concluded that operative banking security mechanism was not only indispensable but also obligatory in banks with a view to curbing and abating e-fraud, impersonation, bank robbery and the likes. In relation to our empirical findings which clearly showed that human induced factors and security mechanisms were key predictors of bank criminalities in the studied area, it is therefore imperious for banks to increase spending on the installation of up-to-date security mechanisms in banks and as well to train and re-train their employees on regular basis. Therefore, bank employees' efficiency and functionality effectiveness of bank security mechanisms are indispensable in order to maintain a very low level of loss of bank and legitimate bank customers' funds to hackers or fraudster.

3.8. Policy Recommendations

Based on the findings from this study, the following policy recommendations are found appropriate to curb the prevailing incidence of bank criminalities across banks in the country:

There is a need for bank administrators to come up with a special control unit with the sole responsibility of day-today monitoring of all on-line activities both external and internal transactions. Also, the activities of this unit should also be closely monitored.

In relation to the aforementioned, there is a need for banks to enlighten their legitimate customers on the effective and safer approach to electronic banking. In fact, banks should take cognisance to explaining in details to their customers on how best to initiate and transact e-banking services. Equally, banks should adopt measures that would make their customers less vulnerable to e-banking frauds.

Also, all banks in the country should be mandated by the appropriate regulatory and monitoring bodies to provide functional CCTV/DVR, especially at automated teller machine centres stationed outside bank location. Furthermore, outdated CCTV/DVR and surveillance cameras should be regularly checked and defaulted ones should be replaced immediately.

3.9. Ethical Consideration

Written permission was sought from the Headquarters of participating banks as a result of the sensitive nature of the information required for the study. This was sought in other to calm the fear of participating bank employees being queried/sacked even making the bank vulnerable to criminality based on the released information. In spite of the ethical clearance, participation in this study was voluntary and based on the consent of all respondents.

Funding: This study received no specific financial support.
Competing Interests: The authors declare that this study has neither been submitted to other journal(s) for publication nor previously published somewhere else.
Acknowledgement: The author acknowledged the self-sacrificing efforts of all research assistants that were engaged in field (data collection) aspect of this study.

REFERENCES

Adams, O.A., 2010. Risk management practices in IS outsourcing: An investigation into commercial banks in Nigeria. International Journal of Information Management, 24(2): 176-180.

Alex, M., 2010. Deterrence: The legal threat in crime control. Chicago, IL: University of Chicago Press.

Aremu, M.A. and Y.A. Ahmed, 2011. An investigation of security and crime management in developing society: The implications for nigeria democratic set-up. International Journal of Academic Research in Business and Social Sciences, 3(1): 390-399.

Cohen, L.E. and M. Felson, 1979. Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4): 588-608.Available at: https://doi.org/10.2307/2094589.

Daniel, O., 2006. Social inequality, collision & armed robbery in Nigerian Cities. British Journal of Criminology, 29: 21-34.

Ebele, J., 2012. Bank robbery and criminality dimension in banking: The offence and the offenders. Security Journal, 10(1): 63-65.

Federal Bureau of Investigation, 2016. A Summary of the Legislation on Cybercrime in Nigeria, Legislative & Government Relations Unit, Public Affairs Department. ATM skimming. Available from https://www.fbi.gov/news/stories/2011/july/atm_071411 [Accessed September 24, 2019].

Hassan, A.B., F.D. Lass and J. Makinde, 2012. Cybercrime in Nigeria: Causes, effects and the way out. ARPN Journal of Science and Technology, 2(7): 626-631.

Maitanmi, O., S. Ogunlere and S. Ayinde, 2013. Impact of cyber crimes on Nigerian economy. The International Journal of Engineering and Science, 2(4): 45–51.

Michael, A., A. Boniface and A. Olumide, 2014. Mitigating cybercrime and online social networks threats in Nigeria. Proceedings of the World Congress on Engineering and Computer Science WCECS 2014, 1: 22–24.

Moses-Òkè, R.O., 2012. Cyber capacity without cyber security: A case study of Nigeria's national policy for information technology (NPFIT). The Journal of Philosophy, Science & Law, 12(1): 1-14.Available at: https://doi.org/10.5840/jpsl20121211.

Ndible, N., 2016. Practical application of cyber crime issues. Available from http://ijma3.org/Admin/Additionals/Cybercrime/Nibal%20Idlebi%20Presentation.pdf [Accessed September 24, 2019].

Okeshola, F.B. and A.K. Adeta, 2013. The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state, Nigeria. American International Journal of Contemporary Research, 3(9): 98-114.

Olumide, O.O. and V.F. Balogun, 2010. E-crime in Nigeria: Trends, tricks, and treatment. The Pacific Journal of Science and Technology, 11(1): 343-355.

Otu, S.E., 2010. Armed robbery and armed Robbers in contemporary Nigeria: The social learning and model visited. International Journal of Criminology and Sociological Theory, 3(2): 438-456.

Parthiban, L. and R. Raghavan, 2014. The effect of cybercrime on a bank's finances. International Journal of Current Research and Academic Review, 2(2): 173-178.

Roberts, E.R., 2013. The social organisation of Armed Robbery. In William A., R. (Ed.).(Deviant Behaviour and social process. Chicago: Rand McNally College. pp: 449 – 513.

Salawu, U.B., 2010. Critical issues in the management of information systems in Nigeria banks: Empirical study. International Journal of Business Information Systems, 3(1): 63 -72.

Shah, S.A., 2012. Assessing the impact of CCTV. (Home, Office Research Study No. 292). London, UK: Home Office Research, Development and Statistics Directorate.

Smith, J., 2012. Crime in developing countries: A comparative perspective. New York: John Wiley and Sons.

Stone, S., 2011. The relation of felonies to environmental factors in indianapolis. Journal of Social Forces, 10: 498-509.Available at: 10.2307/2569897.

Wada, F. and G.O. Odulaja, 2012. Electronic banking and cyber crime in Nigeria - a theoretical policy perspective on causation. African Journal of Computer and ICT, 4(1): 69-82.