Nigerian Journal of Accounting and Finance, Volume 14, Issue 1, 2022

Website: https://www.nijaf.com.ng Email: nijafmautech@gmail.com

BIOMETRIC VERIFICATION NUMBER: A TOOL FOR MANAGEMENT OF FINANCIAL CYBERCRIMES IN THE NIGERIAN BANKING SECTOR

[1]Abubakar Mahmud Bello, [2]Shaibu Babaye Abubakar, & [3]Rafiatu Ahmad Digil

[1]Department of Accountancy, Federal Polytechnic Mubi, Adamawa State

[2]Department of Procurement & Supply Chain Management, Federal Polytechnic Mubi, Adamawa State

[3]Department of Business Administration & Management, Federal Polytechnic Mubi, Adamawa State

[1]Email: Kinggarus43@gmail.com

ABSTRACT

This study assessed Biometric Verification Number: A Tool for Management of Financial Cybercrimes in the Nigerian Banking Sector**.** The objective of the study is to assess whether BVN serves as a tool for management of financial cybercrimes. For the purpose of this study, survey research design was adopted where data were generated from structured questionnaire. 100 respondents were selected in Yola metropolis of Adamawa State, Nigeria. Two hypotheses were formulated for this research. Chi-square at 5% level of significance was used in testing hypothesis 1 while regression was used in testing hypothesis 2 through the use of Statistical Package for Social Sciences (SPSS) version 20. Finding from hypothesis one reveal that there is a high level of significance between BVN and management of financial cybercrimes while hypothesis 2 reveal that BVN has a significant effect on the management of financial cybercrimes by virtue of the analysis showing an R square value of 90.8%. The study recommends that the government should further strengthen the BVN regime in order to effectively tackle the cybercrimes monster that is currently bedeviling the Nigerian financial sector. The CBN should also closely monitor compliance with the standards for the BVN operations in the

Nigerian banking industry contained in its regulatory framework for BVN operations and watch-lists for Nigerian financial system

Keywords: Biometric Verification Number, cybercrimes, regulatory framework, financial system, credit risk

1. INTRODUCTION

The role of biometric verification number in curtailing hazards associated with social security and credit risk cannot be underestimated (Central Bank of Nigeria, 2017). In recent times, biometric technologies have been used to analyze human characteristics as an enhanced form of automation for real time security processes. Overtime, there has been increasing incidences of compromise on our conventional security systems password and pin and thus, there is need for greater security on access to sensitive and also, personal information in the banking system. In the same vein, the extent to which violation in the credit policies and credit monitoring system weakens the financial intermediary system continue to attract empirical and theoretical debate on how well biometric verification system would thwart those issues of default and scam (Integrated Solutions, 2015). In the motive of considering and treating challenges with identity management, the Central Bank of Nigeria (CBN), through the bankers committee in collaboration with all Nigerian banks on February the 14th, 2014, launched a centralized biometric identification system which is known as Biometric Verification Number (BVN).

Fraud is prolific, it is evolving and it is unpredictable. How can security professions manage or overcome such an elusive threat? From Card-Not-Present (CNP) to ATM Fraud to Identity Fraud, the only thing predictable about fraud is its unpredictability. Ransom ware is a prevalent cyber security threat. Threat actors are constantly changing tactics looking for new ways to force ransom payments. With each new emerging ransom ware threat family, the size and scope of threats are more aggressive too. This has led to incredible increases in the average ransoms paid over the past eighteen months. In this session, we will look at recent ransom ware trends, the critical changes to threat actor behaviors, and discuss the strategies and technologies organizations need to defend themselves against this evolving threat.

How organizations think about ransom ware and cybersecurity will play an increasingly vital role in business and productivity (Rose & Walmsley, 2021).

Gartner (2021) asserted that ransom ware attacks have dominated recent headlines. Ransom ware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. These attacks can cost organizations billions of dollars in ransom and lost income, not to mention the risk to human lives. In a ransom ware attack, cyber extortionists deploy malicious software to infiltrate computer systems and encrypt data, holding it hostage until the victim pays a ransom. Ransom ware can have an even bigger impact on an organization than a data breach, but Gartner research estimates that more than 90% of ransom ware attacks are preventable.

Gartner (2021) reported that twenty-seven percent of malware incidents reported in 2020 can be attributed to ransom ware which is a cyber-extortion that occurs when malicious software infiltrates computer systems and encrypts data, holding it hostage until the victim pays a ransom — can have a bigger impact on an organization than a data breach. In the short term, ransom ware can cost companies millions of dollars, and a potentially even greater loss over the long term, impacting reputation and reliability. From top healthcare providers and retailers in the U.S. to insurance providers in the Middle East, ransom ware attackers are proving to be a continuing cyber security threat.

The biometric verification number would give every bank customer, a unique identity across the Nigerian banking industry that can be used for easy identification and verification at point of banking operations. Biometrics refers to identification of an individual based on psychological or behavioral attributes; fingerprint, voice, signature, facial features etc. Biometric verification number (BVN) uses biometric technology to register customers in the financial system. It records these physical features which are unique to individuals; fingerprint and the face (Nigeria Inter-Bank Settlement System, 2015).

The record would be used to identify the person afterwards (Research Clue, 2015). Once a person's biometric has been recorded, and biometric verification number issued, the account would be accessed through the biometric verification number.

The major objectives of the initiative are to protect biometric verification numbers of customers, reduce fraud and strengthen the Nigerian banking system as it also positively affects the economy in general.

In the last few years, both data theft and cyber-crimes have become so widespread that the arrest and prosecution of the suspects have become a major preoccupation of the EFCC (Africa-China Reporting Project, 2022). They are often referred to as Yahoo boys in Nigerian parlance. The groups were a new breed of young people specializing in defrauding Nigerians and foreigners through various online tricks.

Udenze (2014) revealed that banking sector growth is threatened due to high cases of economic and financial crimes; and fraud and money laundering have significant effect on the financial security in the Nigeria banking industry. This problem has negative effect on the reputation of the image of the country, loss of foreign direct investment (FDI), which would also possibly lead to poor infrastructural development, dwindling confidence and distortions in our political as well as financial system, among many other things.

According to Business Email Compromise (BEC) attacks are increasingly used by attackers as a way of targeting organizations. According to Gartner, through to 2023, BEC attacks will continue to double each year to over $5 billion and lead to large financial losses for enterprises. How can CISOs respond to this ever-increasing threat? Join this exclusive panel for unique insight into:

- What a successful compromise of an organization's email system looks like
- Strategies to detect and respond to Business Email Compromise attacks
- Why education and awareness training are still crucial and how to deliver it in a way that works.

The persistent re-occurrence of e-fraud between 2020 and 2021 made the Central Bank of Nigeria to issue a fraud alert about the activities of cyber-criminals who took advantage of the coronavirus pandemic to defraud citizens. According to the Apex bank, cyber-criminals took advantage of the COVID-19 pandemic by sending messages to customers claiming to be from the government with offers of financial palliative to defraud citizens and steal sensitive information or gain unauthorized

access to computers or mobile devices using different techniques. In view of these crises as a result of crimes perpetuated by cyber thieves, the mandatory biometric verification number exercise, embarked on by various banks nationwide also to temporary congestions in banking halls. The inflow and outflow of money in the country is carried out through the banking sector, but growth in this sector has been reduced due to high cases of cyber thieves, economic and financial crimes; fraud and money laundering in Nigeria banking industry (Udenze, 2014). Building a robust security ecosystem is vital for organizations in the era of accelerating digital business, given that each security risk represents a strategic shift in the security world that will have broad industry impact and significant potential for disruption.

It is against this background that this study seeks to examine if there is a significant relationship between BVN and financial cybercrimes, with data from some banks. Hence there is the need for a comprehensive study to find out if BVN can serve as a tool for management of financial cybercrimes in Nigeria.

The Study Objectives

This study is aimed at determining:

i. The level of significance between Biometric verification number (BVN) and management of financial cybercrimes.
ii. Whether BVN serves as a tool for management of financial cybercrimes in the Nigerian banking sector.

To achieve the above objective, the following hypotheses were formulated to guide the research:

H_{o1}: The level of significance between BVN and management of financial cybercrimes is low.

H_{o2}: BVN does not serve as a tool for management of financial cybercrimes in the Nigerian banking sector.

2. LITERATURE REVIEW

Ajijola (2015) conducted a research which revealed that banks have invested heavily in security and have shifted focus to systems that detect abuse and intrusion by

looking at the data and application layer systems that detect abuse and intrusion. The study concluded that the level of significance between BVN and cybercrimes is high and that the financial system survives on confidence that requires knowing the identity of who participates in it's on and off line transactions, hence the Banks need this authentication information (BVN).

Omodunbi, Odiase, Olaniyan and Esan (2016) carried out a research on cybercrimes in Nigeria with particular interest in the prominent cybercrimes carried out in the various sectors in Nigeria and presented a brief analysis of cybercrimes in tertiary institutions in Ekiti-State. The study revealed that 88% of the students that participated in the analysis are victims of phishing. Majority disclosed that they receive false mails and text messages which has in turn led to the loss of money and disclosure of private in-formation in some cases.

Orji (2019) reported that Cybercrimes that target electronic banking and payment services generally reduce consumer trust in electronic transactions and also impedes the adoption and penetration of electronic banking and payment services as well as e-commerce. This also has the effect of limiting the social and economic devel-opment prospects of information communication technologies in developing countries such as Nigeria. More importantly, the Nigerian Cybercrime Advisory Council which is established under section 42(1) of the Nigerian Cybercrimes Act has powers to formulate guidelines for the implementation of the Act. In this regard, the Council has made guidelines that will impose a greater or strict liability regime on banks and financial institutions under section 19(3) of the Cybercrimes Act, so that they can have a higher degree of liability for the breach of consumer data.

Project beam (2022) conducted a research and collected data on number of staff involved in banking sector, total amount involved in fraud, actual amount lost to fraud and number of fraud cases. The study tested for significant difference in these variables in periods before (2010-2014) and after (2015-2017). The introduction of BVN in the banking sector and the findings showed that there is significant reduction in the total amount involved in fraud in the banking system in periods after BVN introduction; There is no significant reduction in the actual amount lost to fraud in the banking system in periods after BVN introduction; There is no significant reduction in the number of staff involved in fraud in the banking system in periods after BVN introduction. The study concludes that BVN scheme in Nigeria has been

partially effective in tackling financial crimes and preventing fraudulent activities in the Nigerian banking system.

Ater, (2023) reported that statistics show that Nigeria loses about N127 Billion annually to cybercrime. This figure represents 0.8% of the country's Gross Domestic Product (GDP). For instance, in 2015, the Information Security Society of Nigeria (ISSAN) revealed that about 25 per cent of cybercrime in Nigeria are unresolved and 7.5% of the world hackers are Nigerians. The EFCC also reported in 2014 alone that customers in Nigeria lost approximately six billion naira to cybercriminals. Similarly, the CBN in 2015 reported that 70 per cent of attempted or successful fraud/forgery cases in Nigeria's banking sector were perpetrated via electronic channels. Banks in Nigeria have lost approximately 159 billion naira to electronic frauds and cybercriminals between the years 2000 and 2013 and the impact on the nation's economy as well as cashless policy are significant. Cybercrime has been outlawed by the Cybercrimes (Prohibition, Prevention Etc.) Act 2015, it therefore means that perpetrators of same may invariably engage in an organized group to perpetuate incidence of cybercrimes; fraud; forgery covered under section 15(6) above. Cybercrime can be interpreted to come under "any other criminal act." used therein.

Consequently, proceeds from acts perpetrated by cybercriminals are unlawful and when they are laundered, they are held to have committed the offence of money laundering. Anyone who violates section 15(2) of the Act is liable on conviction to a term of not less than 7 years but not more than 14 years imprisonment but where it is a body corporate, liability is on conviction to- (a) a fine of not less than 100% of the funds and properties acquired as a result of the offence committed; and (b) withdrawal of license.

According to Ater, (2023), the following are the most common types of cybercrimes:

Fraud: Is a general term used to describe a cybercrime that intends to deceive a person in order to gain important data or information. Fraud can be done by altering, destroying, stealing, or suppressing any information to secure unlawful or unfair gain.

Scamming: Scam happens in a variety of forms. In cyberspace, scamming can be done by offering computer repair, network troubleshooting, and IT support services,

forcing users to shell out hundreds of money for cyber problems that do not even exist. Any illegal plans to make money falls to scamming.

Computer Viruses: Most criminals take advantage of viruses to gain unauthorized access to systems and steal important data. Mostly, highly-skilled programs send viruses, malware, and Trojan, among others to infect and destroy computers, networks, and systems. Viruses can spread through removable devices and the internet.

Ransom ware: Is one of the most destructive malware-based attacks. It enters your computer network and encrypts files and information through public-key encryption. In 2016, over 638 million computer networks are affected by ransom ware. In 2017, over $5 billion is lost due to global ransom ware.

Distributed Denial of Service attack (DDoS): is one of the most popular methods of hacking. It temporarily or completely interrupts servers and networks that are successfully running. When the system is offline, they compromise certain functions to make the website unavailable for users. The main goal is for users to pay attention to the DDoS attack, giving hackers the chance to hack the system.

Botnets: Are controlled by remote attackers called "bot herders" in order to attack computers by sending spams or malware. They usually attack businesses and governments as botnets specifically attack the information technology infrastructure. There are botnet removal tools available on the web to detect and block botnets from entering your system.

Spamming: Uses electronic messaging systems, most commonly emails in sending messages that host malware, fake links of websites, and other malicious programs. Email spamming is very popular. Unsolicited bulk messages from unfamiliar organizations, companies, and groups are sent to large numbers of users. It offers deals, promos, and other attractive components to deceive users.

Phishing: Act like a legitimate company or organization. They use "email spoofing" to extract confidential information such as credit card numbers, social security number, passwords, etc. They send out thousands of phishing emails carrying links to fake websites. Users will believe these are legitimate, thus entering their personal information.

Social Engineering: Is a method in which cybercriminals make a direct contact with you through phone calls, emails, or even in person. Basically, they will also act like a legitimate company as well. They will befriend you to earn your trust until you will provide your important information and personal data.

Malvertising: Is the method of filling websites with advertisements carrying malicious codes. Users will click these advertisements, thinking they are legitimate. Once they click these ads, they will be redirected to fake websites or a file carrying viruses and malware will automatically be downloaded.

Cyber stalking: Involves following a person online anonymously. The stalker will virtually follow the victim, including his or her activities. Most of the victims of cyber stalking are women and children being followed by men and pedophiles.

Software Piracy: The internet is filled with torrents and other programs that illegally duplicate original content, including songs, books, movies, albums, and software. This is a crime as it translates to copyright infringement. Due to software piracy, companies and developers encounter huge cut down in their income because their products are illegally reproduced.

Child Pornography: Porn content is very accessible now because of the internet. Most countries have laws that penalize child pornography. Basically, this cybercrime involves the exploitation of children in the porn industry. Child pornography is a $3-billion-a-year industry. Unfortunately, over 10,000 internet locations provide access to child porn.

Cyber bullying: is one of the most rampant crimes committed in the virtual world. It is a form of bullying carried over to the internet. On the other hand, global leaders are aware of this crime and pass laws and acts that prohibit the proliferation of cyber bullying.

Hacking: This is simply any unauthorized access of a computer system. Sometimes, hacking can be fairly harmless, such as rewriting sections of an existing software program to allow access to features the original designer did not intend. While this is technically a violation of the Terms of Service agreement, it is not exactly a prosecutable offense but is still considered hacking. Hacking is probably one of the most broadly used forms of cybercrime, but not all hackers are criminals. Some

hackers often referred to as "white hat" hackers, are hired by software companies to find flaws in their systems so they can fix them before "black hat" or criminal hackers do.

Identity Theft: Identify theft is a specific form of fraud in which cybercriminals steal personal data, including passwords, data about the bank account, credit cards, debit cards, social security, and other sensitive information. Through identity theft, criminals can steal money. According to the U.S. Bureau of Justice Statistics (BJS), more than 1.1 million Americans are victimized by identity theft (Ater, 2023).

Over the years, some frameworks were put in place by the government to tackle the issue of cybercrimes in Nigeria. Such frameworks include but are not limited to:

Cyber security Act 2015

The Cybercrimes Act 2015 is the first legislation in Nigeria that deals specifically with cyber security. Passed in May 2015, it gives effect to the 2011 ECOWAS Directive on fighting cybercrime and is broad in its scope. The Act charges the offices of the National Security Advisor (NSA) and the Attorney-General of the Federation (AGF) with coordinating its enforcement and creates the multi-agency Cybercrime Advisory Council (the Council) and the National Cyber Security Fund (the Fund) to be overseen by the NSA. Section 38 requires service providers to keep all traffic data and subscription for a period of at least two years. Further, service providers are required to turn over such information to law enforcement agencies and failure to comply with either attracts a fine of 7m naira (Ater, 2023)..

Theoretical Framework

The selected theory for this study is fraud diamond theory which was first presented by Wolfe and Hermanson in the CPA Journal in December 2004. However, it is essential to highlight the interconnectivity between the Fraud Triangle Theory (FTT) and the Fraud Diamond theory (FDT).

Fraud Triangle Theory: In 1950, Donald Cressey, a criminologist, started the study of fraud by arguing that there must be a reason behind everything people do. Questions such as why people commit fraud led him to focus his research on what drives people to violate trust? He interviewed 250 criminals in a period of 5 months

whose behavior met two criteria: (i) initially, people are accepting responsibilities of trust in good faith, and (ii) circumstances make them violate the trust. He relates that three factors (pressure, opportunity, and rationalization) must be present for an offense to take place.

Fraud Diamond Theory: Abdullahi and Mansor (2015) reported that the FDT is viewed as an expanded version of the FTT. In this theory, an element named capability has been added to the three initial fraud components of the FTT. Wolfe and Hermanson (2004) argued that although perceived pressure might coexist with an opportunity and a rationalization, it is unlikely for fraud to take place unless the fourth element (i.e., capability) is also present. In other words, the potential perpetrator must have the skills and ability to commit fraud. They also stated that the four sides of the fraud diamond actually overlap each other and that the primary lesson of the fraud diamond indicates that assessing capability to commit fraud separately in any fraud risk assessment process is key. This moves beyond viewing of fraud opportunity in terms of environmental or situational factors as is currently been practiced.

This paradigm was adopted because conscious capacity must be built in the area of fraud perpetration before it can be used for committing any fraud.

3. METHODOLOGY

This study adopts survey research design as data were obtained mainly from primary source. Regression analysis is a method used in statistics that helps to identify which variables exert an impact on a particular experiment topic. The process helps determine which factors matter the most, which are to be ignored, and how the factors influence each other. Research design described how the dependent variable is affected by the independent variables

The population adopted for the study consists of 10 staff each from Ecobank, First Bank, Zenith Bank, Skye Bank, Keystone Bank, GT Bank, Union Bank, UBA, Fidelity Bank and Access Bank respectively which gives a total of 100, all in Yola Adamawa State. The sampling technique used for the study is the simple random sampling.

For the regression analysis, a model was formulated for testing the hypothesis. The model is:

$$MgtFinCybercrimes_0 = \alpha + \beta_0 BiometrVerificatnNumber_0$$

Where: $MgtFinCybercrimes_0$ = Management of financial cybercrimes

α = Intercept of regression model

$\beta_0 BiometrVerificatnNumber_0$ = Biometric Verification Number (BVN)

μ = Error

4. RESULTS AND DISCUSSION

This part presents the results from the data analysis. The results and the inferences taken from the hypotheses investigated are presented in this section. To determine the relationship between the regressors and the dependent variables, Chi Square was used in testing hypothesis 1 while Regression analysis was used in testing hypothesis 2 on the Statistical Package for Social Sciences (SPSS).

Test of Hypothesis 1

Table 1. Case Processing Summary

	Valid N	Missing N	Total
Is the level of significance between BVN and management of financial cybercrimes low?	89	11	100

Source: Authors' Analysis (2022)

Table 2. BVN Cross tabulation

	High	Low	Total
Senior Staff	39	1	40
Middle Level Staff	45	4	49
Total	84	5	89

Source: Authors' Analysis (2022)

Table 3. Chi-Square Tests

	Value	Df	Significance
Pearson Chi-Square	4.4394[a]	1	0.000
Likelihood Ratio	4.5038	1	0.000
Linear-by-Linear Association	1.5484	1	0.000
N of Valid Cases	89		

Source: Authors' Analysis (2022)

The value of the test statistic is 4.4394.

The 1st column has cell count greater than or equal to 5 while 2nd & 3rd have less: so this assumption (hypothesis) was not met.

Because the test statistic is based on a 2x2 cross tabulation table, the degrees of freedom (df) for the test statistic is df = (R - 1)*(C - 1) = (2 - 1)*(2 - 1) = 1*1 = 1

The corresponding p-value of the test statistic is $p = 0.000$.

DECISION

Since the p-value is less than our chosen significance level ($\alpha = 0.05$), we therefore reject the null hypothesis. Rather, we conclude that the level of significance between BVN and management of financial cybercrimes is high.

Test of Hypothesis 2

For testing the second hypothesis, the collected data was analyzed using computer programs particularly the Statistical Package for Social Sciences (SPSS) version 20 for easy analysis and interpretation of results.

Table 4. Regression Analysis for the Model

Variables		B	B value	T	P	
Biometric Number	Verification	0.872	0.953	31.107	0.000	
R						0.953
R Square						0.908
Adjusted R Square						0.907
F						967.633
Significance						0.000
Constant						0.230

Source: Authors' Analysis (2022)

This table indicates that the regression model predicts the dependent variable very well. The regression Row "Sig" column shows that the statistical significance of the regression model was run. Here, P‹0.0005, which is less than 0.5, and indicates that, overall, the regression model statistically significantly predicts the outcome variable that is (it is a good fit of the data).

The table also provides the R and R^2 values. The R value represents the simple correlation and is 0.953 (the 'R' column), which indicates a high degree of correlation. The R^2 value (the R square column) indicates how much of the total variation in the dependent variable (management of financial cybercrimes) can be explained by the independent variable (BVN).

Lastly, the table provides the necessary information to predict management of financial cybercrimes from bank verification number, as well as determine whether BVN contribute statistically to the model (by making reference to the "Sig" column).

The results in the table above are substituted into the regression function in order to appreciate the analysis:

$MgtFinCybercrimes_0 = \alpha + \beta_0 BiometrVerificatnNumber_0$

$MgtFinCybercrimes_0 = .230 + .872$

Findings from testing hypothesis 1 revealed that there is high level of significance between BVN and management of financial cybercrimes by virtue of a P-value less than 0.05. This is in line with Ajijola (2015) whose study revealed that the level of relationship/significance between BVN and cybercrimes is high.

Findings from testing hypothesis 2 revealed that very vital points are obvious from the results of the analysis. The results indicate a direct relationship between Biometric verification number (.872) and the management of financial cybercrimes.

The overall relationship between the explanatory variables: BVN and the explain variable: management of financial cybercrimes as suggested by the functional analysis is very high as revealed by the model R which is about 95.3% i.e. R= 0.953. The analysis further revealed an R square of .908. This means that the explanatory variable only explained about 90.8% of variations in management of financial cybercrimes, and as such this implies that the remaining 9.2% changes are attributable to other variable(s) not included in this model.

The findings of hypothesis 2 are in line with that of Omodunbi et al (2016), which revealed that BVN is very essential in the management and tackling of financial cybercrimes through email inspection and use of network intrusion detection system.

The findings also correspond to Orji (2019) who revealed that the CBN has exercised its powers to regulate the banking and financial sector in order to make regulations in order to strengthen the consumer protection regime under the Cybercrimes Act by using the BVN.

Project beam (2022) also discovered that BVN scheme in Nigeria has been partially effective in tackling financial crimes and preventing fraudulent activities in the Nigerian banking system and the study suggested that; The CBN should continue to ensure that financial institutions have thorough knowledge of their customers and their businesses and that banks operating in Nigeria are not used for the movement of illicit funds across the globe.

5. CONCLUSIONS AND RECOMMENDATIONS

Based on the findings of the study, it is concluded that there is a high level of significance between BVN and management of financial cybercrimes.

It was also concluded that BVN taken as the independent variable significantly affects the management of financial cybercrimes by virtue of the regression model (R coefficient) which shows a good level of prediction (95.3%) and that 90.8% change in the management of financial cybercrimes is caused or predicted by BVN. Therefore, the variable added significantly to the prediction of cybercrimes, meaning that BVN and the management of financial cybercrimes are positively correlated.

By virtue of the study revealing a high level of significance between BVN and management of financial cybercrimes, and that BVN serves as a significant tool for the management of financial cybercrimes, the study recommends that:

The government should further strengthen the BVN regime in order to effectively tackle the cybercrimes monster that is currently bedeviling the Nigerian financial sector.

The CBN should closely monitor compliance with the standards for the BVN operations in the Nigerian banking industry contained in its regulatory framework for BVN operations and watch-lists for Nigerian financial system.

REFERENCES

Abdullahi, R. & Mansor, N. (2015). Fraud triangle theory and fraud diamond theory: Understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Sciences 5, (4), pp. 38–45 https://www.hrmars.com*

Africa-China Reporting Project. (2022). *Data for fraud: How the biometric system exposes Nigerians to cyber thieves.* https://africachinareporting.com/data-for-fraud-how-biometric- system-exposes-Nigerians-to-cyber-thieves

Ajijola, A. (2015). Biometric verification number (BVN) & Cybercrime in Nigeria. *https://www.linkedin.com/pulse/bank-verification-number-bvn-cybercrime-nigeria-abdul- hakeem-ajijola*

Ater, S.V. (2023). *Legal Framework for the Prohibition of Cybercrime in Nigeria*. *https://sabilaw.org/legal-framework-for-cybercrime/*

CBN, (2017). *Regulatory Framework for Biometric verification number (BVN) Operations*.https://www.cbn.gov.ng/Out/2017/BPSD/Circular%20on%20the%20

Regulatory Framework for BVN Watchlist for Nigerian FinancialSystem.pdf Gartner Research (2021). *5 Must-Read Ransomware and Cybersecurity Articles. https://www.gartner.com/smarterwithgartner/5-must-read-ransomware-and- cybersecurity-articles/*

Gartner Research, (2021). *6 Ways to Defend Against a Ransomware Attack. https://www.gartner.com/smarterwithgartner/6-ways-to-defend-against-a-ransomware- attack/*

Integrated Solutions (2015). *BVN Enrolment.* https://oisservices.com/bvn.php

NIBSS, (2015). *Biometric verification number (BVN)*. https://www.nibss-plc.com.ng/services/bank- verification-number-bvn

Omodunbi, B. A., Odiase, P. O., Olaniyan O. M & Esan A. O. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention. *FUOYE Journal of Engineering and Technology, 1, (1), 2579-2591*

Orji, U.J (2019). Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria. http://doi.org/10.5334/tilr.137

Projectbeam (2022). *The effect of biometric verification number (bvn) on fraud prevention in Nigeria banking industry and Nigeria's economy.* https://projectbeam.com.ng/the- effect-of- bank-verification-

number-bvn-on-fraud-prevention-in-nigeria-banking-industry-and-nigerias-economy-2/

Research Clue. (2015): *Biometric verification number: Implication on the Nigerian economy and banking sector*. https://nairaproject.com/projects/1985.html.

Rose, A. & Walmsley, M. (2021). BEC attacks: Detection and response. *https://www.cybered.io/webinars/bec-attacks-detection-response-w-2739*

Udenze, O. (2014). The effect of corruption on foreign direct investments in developing countries. *https://digitalcommons.iwu.edu/parkplace*

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