

Effect of Bank Verification Number on Fraud Management of Selected Commercial Banks in Ebonyi State, Nigeria

Robert Azu Nnachi¹, Benedette Nneka Okezie¹ Ogbonnaya Okpara Elechi², Emmanuel Nwogboji,¹ Ngozi Franca Iroegbu³, Hyginus Emeka Nwosu³, Oladele Rotimi⁴, Kanu Catherine Chiugo^{5*}

¹Department of Accountancy /Banking & Finance , Faculty of Management and Social Sciences, Alex Ekwueme Federal University, Ikwo, Ebonyi State Nigeria.

²Department of Accountancy; Faculty of Management, Ebonyi State University Abakaliki. Ebonyi State Nigeria.

³Department of Business Administration, Faculty of Management and Social Sciences, Alex Ekwueme Federal University, Ikwo, Ebonyi State Nigeria.

⁴Department of Accounting, Federal University Oye-Ekiti, Ekiti State Nigeria.

⁵Department of Business Education, Faculty of Vocational and Technical Education, University of Nigeria, Nsukka, Nigeria.

Correspondence: Kanu Catherine Chiugo, Department of Business Education, Faculty of Vocational and Technical Education, University of Nigeria, Nsukka, Nigeria. E-mail ID: catherine.kanu@unn.edu.ng ORCID: 0000-0002-5059-6266

Abstract

This study examined the effect of bank verification number (BVN) on fraud management of selected commercial banks in Ebonyi state. The study highlighted on the effectiveness of BVN in curbing identity theft and ensuring safety of depositors' fund in the selected banks. The study adopted a survey research design and Primary data for this study were obtained through questionnaires, which were administered to 50 management staff of the eight (8) selected banks. However, out of the 50 copies of the questionnaires that were distributed, 35 copies were returned and used for the analysis while 15 copies were both invalid and not returned. The data obtained were descriptively analysed using tables, percentages and mean. The hypothesis was tested using simple linear regression. The findings indicates that BVN has a significant positive effect on reduction of identity theft and safety of depositors' fund ($r = 0.136$; $t = 6.491$; $p = 0.000 < 0.05$). The study concludes that the adoption of biometric system through BVN scheme has significant effect on fraud management of the studied commercial banks. It also recommends that biometric system should be extended to banking operations like internet banking, mobile banking, ATM banking and Point of Sales (POS) due to its effectiveness in reducing fraud in Nigerian banking sector.

Keywords: Bank Verification Number, Biometric, Fraud Management, Identity Theft, Depositors Fund

INTRODUCTION

Banking industry plays a very vital role in the development and sustainability of economic growth in both developed and developing countries (Adeyemo, 2012). According to Uzoma (2010), a bank is an establishment for lending, issuing, borrowing, exchanging and safeguarding money. However,

the ineffectual authentication techniques in Nigeria induce fraudsters and scammers to manipulate and claim identities that are different from who and what they are; as well as using various sophisticated techniques to perpetrate financial and identity fraud, which to a very large extent, hinders the performance of commercial banks in Nigerian banking sector (Idolor, 2010). Ratha, Chukkerur, Connell and Bolle (2007) argued that the true identity of a person visiting sensitive institutions like banks can only be accurately identified using multifactor authentication system—combination of identification cards, passwords/PINs and biometric system. A biometric system uses a non-replicable data of an individual to authenticate such person and his/her address. In exercise of the power conferred on the Central Bank of Nigeria (CBN) in section 2(d) and 47(2) of CBN Act (2007) — to promote a sound financial system as well as facilitate the development of efficient and effective systems for the settlement of transactions in Nigerian banking sector— CBN launched a biometric technique known as bank verification number (BVN) in February, 2014. Orji (2014) opined that the primary essence of implementing BVN is to help commercial banks in the protection of depositors' funds as well as reduce financial crimes in the Nigerian banking sector. In addition, Ehi (2015) opined that BVN is part of the general policies of the financial sector strategy (FSS) designed to make sure that Nigeria becomes one of the largest economies in the world by the year 2020. Biometric BVN scheme was designed to revolutionize the Nigerian commercial banks, cut all financial malpractices and strengthen the entire banking sector (Ogunleye, Fashoto, Andile & Ogunde, 2017).

Bamidele (2015) argued that identity management has not thrived in the Nigeria banking sector unlike other countries like Brazil, Australia, United states, Mexico etc., where biometric identification techniques have been adopted because of their effectiveness in identity security. Nevertheless,

despite that Nigerian government has implemented numerous statutory regulations to curb frauds in banking sector (ranging from criminal and penal code Act, Companies and Allied Matter Act, 1990; Banks and other Financial Institution Act, 1990; Central Bank of Nigeria Act, 1991; Nigeria Deposit Insurance Corporation Act, 1988; Financial Malpractices in Banks Act, 1994, and other financial security measure), financial malpractice still remains an issue of major concern in Nigerian banking sector. In the report from Nigeria Interbank Systems (NIBSS), it was stated that Nigerian banks lost a total of N159 billion to cybercrime between 2000 and 2013. This represents a loss of roughly N33 million per day or approximately N12 billion per year, which more than average took place from 2010 when the internet became a booming tool for identity fraud (Chima, 2014). Similarly, the annual reports of Nigerian Deposit Insurance Company (NDIC) shows there was 182.77% increase in successful fraud cases in Nigerian commercial banks between 2010 and 2014 (James, 2014). Such increase shows a high incidence of compromise on the traditional security systems like identification cards, passwords and PINs. There is a large and growing body of evidences (Pooe & Labucshague, 2011); Adewale, Ibidumi & Badepo, 2014; Imuetinyan, 2010) which demonstrate that optimization of traditional authentication system or adoption of new, more effective system is crucial for curbing identity theft as well as ensure adequate security of depositors fund in commercial banks. Therefore, Biometric Bank Verification Number (BBVN) appears to be an effective authentication system for adequate compliance with the CBN policy on Know Your Customer (KYC); which is enshrined in CBN AML/CFT Manual, 2009. The central aim of this study is to investigate the effect of BVN on fraud management in Nigeria banking sector. Specifically, the study will examine the effectiveness of BVN in curbing identity theft and safety of depositors' funds in the selected commercial banks within Ebonyi state.

OBJECTIVES OF THE STUDY

The following specific objectives of the study

1. To examine the effectiveness of BVN in curbing identity theft in the studied banks
2. To ascertain the extent to which BVN serves as an effective tool for safety of depositors' fund in the studied banks
3. To establish the nature of relationship between BVN and operational efficiency in the studied banks

REVIEW OF RELATED LITERATURE

Conceptual Review

Biometric Technology in the Nigerian Banking System

In this highly interconnected information era, adequate identity management can only be guaranteed using a robust technique such as biometric system (Venkatraman & Delpachitra, 2008). Biometric is derived from the Greek

words bio (meaning life) and metro (meaning measurement). Bolle et al (2003) defined biometric as a systematic process of identifying, verifying and validating a person and his/her identity based on physiological or behavioral traits. These traits include fingerprints, finger vein patterns, iris, and voice recognition. Similarly, biometric is an approach that automatically recognizes the measurable physiological and behavioral features of a living person. These characteristics are unique for every individual and cannot be forged or replicated. The nonreplicable nature of biometric verification and authentication system makes it a commonplace in sensitive areas like immigration control, law enforcement, forensic studies and investigations as well as banking sector (Craven & Eloff, 2015; Capoor, 2006).

Several banks across the globe have adopted biometric technique for effective identity security as well as ease authentication of customers before, during and after banking operations. Among the total banks that utilize biometric techniques in their banking operations as at 2012, Japan has about 15 million customers using biometric authentication for banking transactions. Banks in Mexico, South America, Africa, and the Middle East are also moving towards the use of biometric identification technology because of its ability to offer more security than the personal identification numbers (PINs) and passwords (Hosseini & Mohammadi, 2012). Although biometric as a reliable technology for identity management has thrived in many industries, the rate of its adoption in banking industry is still low. Hosseini & Mohammadi (2012) further claimed that only 121 banks in the world use biometric technology in their operations as at 2012. Among which 52% are located in Asia, 32% in America, 9% in Europe, 6% in Africa, and 1% in Australia.

The purpose of adopting a biometric system into banking sector through BVN scheme is to use biometric information of bank clients as a means of identifying and verifying all individuals that have accounts in any of the Nigerian commercial banks, and subsequently authenticate customers' identity at various banking transactions. Though BVN is not 100% perfect, but it is currently more effective than using only password and PIN (Ehi, 2015). However, Nigeria banking industry does not fully migrate from traditional approach to pure biometric approach, but the combination of the two approaches known as two-factor authentication system. According to Conroy (2017), a two-factor or multifactor authentication system is the most reliable and secured method of preventing identity theft in the banking industry. The two-factor system implemented in the Nigerian banking system captures the customers' fingerprints, facial structures, and signatures together with documents like NEPA bill, ID cards, driving license and voter's card. These modalities are coded into numerical figures known as the Bank Verification Number, which is issued to every bank customer at the end of the biometric enrolment (Bamidele, 2015).

Application of Biometrics in Banking Operations

Biometric authentication offers a natural and most reliable solution to the problem of identity theft (Akinwesi, Uzoka, Okwundu, & Fasholo, 2016). Since the biometric identifiers

are inherent to an individual, it is more difficult to manipulate, share, or forget the traits. Hence, biometric traits constitute a strong and reasonably permanent link between a person and his identity. Biometric authentication system is gradually replacing the existing conventional identity techniques in the banking industries. Biometric system can be applied in various banking operations and services to better protect accounts and personal information of customers (Imuetinyan, 2010). Banks and other financial institutions authenticate their clients through fingerprint/thumbprint. This biometric technique is suitable for authenticating bank customer, especially when the cashiers/tellers are under pressure. In addition, fingerprint or thumbprint ensures reliable and adequate identity security by reducing impersonations in sensitive institutions like banks. For instance, the valid identity and address of a bank customer can be authenticated by a bank personnel using a thumbprint scanner that matches the customer's biometric template in the bank's biometric database. If the customer's finger vein matches with the biometric details installed in the database during biometric enrolment process, the customer will be allowed to proceed with his/her banking transactions (Jain, 2004).

In the same vein, the adoption rate of biometric techniques in ATM banking in some developed countries is significantly on the rise. Based on evidence from researchers, most banks in Brazil do not use ATM card but rely on biometric thumbprint for self-authentication during ATM banking. However, some countries use both bank cards and biometric modalities like iris and facial recognition and fingerprints. The combination of bank cards and biometric techniques in ATM banking ensures flexibility, compactness, and accuracy as well as reduce impersonations in ATM banking (Hosseini & Mohammadi, 2012). Similarly, modern technological gadgets like laptops, computers and phones now have webcams and thumbprint scanners that make it easier for banks to adopt biometric system in mobile and online banking services (Venkatraman, & Delpachitra, 2008).

During banking transactions or before a bank client gains access to his account, banks that use biometric authentication system require the customer to present their biometric details first. Most banks that use two-factor or multi-factor authentication techniques require both biometric authentication and other traditional authentication modalities like password, pin, NEPA bill, birth certificate, etc., to avoid impersonation. Two-factor/Multi-factor authentication system helps banks and other financial institutions to adhere to the CBN policy on "Know Your Customer" and as well protect customers' identities and other personal information from being compromised by cyber criminals and imposters in attempt to obtain sensitive customers' information to perpetrate financial crimes (Conroy, 2017).

Similarly, online and mobile banking is growing rapidly across the globe. According to Juniper Research (2018), 800 million bank customers are using mobile banking as at 2014 and it's expected to exceed 1.75 billion by 2019; which represents 32% of the entire global adult population. Such implies that about 68% global adults lack trust over the security of their funds and personal information during online and mobile transactions. However, the application of

multifactor authentication system appears to be an effective tool that ensures adequate security of depositors fund and other relevant personal information.

Theoretical Framework

Scholars have made serious attempts to connect several factors and conditions that determine the adoption of modern technologies into comprehensive theories. For instance, the **Theory of Reasoned Action (TRA)** developed by Martin Fishbein and Icek Ajzen in 1975 suggests that an individual's actual behavior is contingent on his/her behavioral intention. It further suggests that a person is influenced by two factors: attitude towards the behavior and subjective norm (Fishbein & Ajzen, 1980). The attitude of a person is the positive or negative feelings about performing a target behavior. On the other hands, subjective norm is an individual's perception on what other people think about a target behavior. Again, the **Theory of Planned Behavior (TPB)** propounded by Icek Ajzen in 1985 holds that behavior is not absolutely voluntary and controlled, but can be deliberate and planned. This theory added a third factor—perceived behavioral control—to the two factors in the theory of reasoned action (Ajzen 1985, 1991). As reviewed by various scholars (Davis 1989, Davis, Bagozzi & Warshaw, 1989), technology acceptance model (TAM) was built upon TRA and TPB. Technology acceptance model holds that the acceptability of any information system is influenced by two main factors: perceived usefulness and perceived ease of use. Perceived usefulness is the degree to which an individual believes that their job performance will be enhanced by using a particular system while perceived ease of use is the degree to which an individual believes that using a particular system will be facile (Davis et al. 1989). Hauser & Shugan (1980) argued that perceived ease of use influences perceived usefulness since the easier the usage of a system, the higher the accomplishment; and the more clumsy a system, the less work the individual will be able to finish. Nevertheless, Davis et al (1989) holds that perceived usefulness and perceived ease of use are the two factors that shape the attitude of an individual towards the adoption of any information system. Therefore, these theories (reasoned action and planned behavior) justified this study in the sense that, even if some banks failed to adopt biometric authentication technique in the short run, the probability that they will implement it in the long run is high; especially when they discover its effectiveness in identity and information security, such that identity theft will be reduced and depositors' funds will be properly secured.

Empirical Literature Review

Craven and Eloff (2012) carried out a study on the occurrence of fraud in the micro lending industry and present a pilot biometrics project conducted in Rustenburg with a small group of micro lenders. Data for the study were generated through a series of interview with leading figures in the micro lending and broader financial arena. From the interview, it was identified that South Africa ID book is easily forged. It was further estimated that 20% of all fraud is conducted using illegitimate ID book, while 30% of all fraud is conducted through impersonation, which is the passing of a legitimate ID book by someone who is not the legal holder.

However, the concludes that the effect of biometric system in money lending industry in South Africa is positive and as such, ensures security of funds.

Adewale, Ibidumi, and Badepo, (2014) carried out an empirical study on biometric enabled e-banking in Nigeria. The researchers' evaluation captures the factors influencing the perception of the bank management and ATM users. The study was based on a survey of 740 respondents cutting across different age group and educations background. Descriptive statistic and t-test analysis of the survey showed that management and customer strongly support the adoption of biometric ATM in Nigeria due to its effectiveness in securing their identity and personal information as well as their deposited funds. The findings of study provide a platform to enhance the integration of biometric into identity management.

Imuetinya (2010) reviewed the implementation of an efficient biometric authentication framework for Nigeria banking systems. Data for the study was collected via interview and questionnaire. The study was based on a survey of 100 respondents who were issued questionnaires. And the result of the survey conducted suggested that more efficient biometric framework will ensure more secured banking system in Nigeria. The study concludes that banking industry in Nigeria has been responsive to better technology as individuals (customers) that depend on banking institution for various financial transactions tend to increase on daily basis.

Hosseini and Mohammadi (2012) reviewed biometric applications in banking industry in the world to determine the level of frauds and security breaches in traditional security systems such as identification cards and passwords/PIN. The researchers employed secondary data obtained from 121 banks across the globe, which are identified to be using biometric techniques in various operations as at 2012. The findings of the study show that biometric technology is a perfect solution to defeat financial and identity fraud in the

banking industry; and further recommends that biometric model could help banks to provide convenient and more secured banking services to customers.

From the above reviewed studies, it's obvious that none of the authors who evaluated the effectiveness of biometric techniques on banking operations in different banking industries was motivated to study the effect of BVN, as a biometric authentication scheme, on fraud management of some selected banks in Nigerian banking industry. This lacuna necessitated this study. Hence, the researcher is motivated to look critically at this angle using controlled variables like safety of depositors' fund and rate of identity theft.

METHODOLOGY

The study adopted a survey design using questionnaire. The questionnaire administered was designed to reflect five (5) point likert scale. Out of fifty (50) copies of questionnaire distributed to management staff of the selected commercial banks, thirty five (35) representing about 70% were received. The choice of the management staff is because, in any organization, issues and policies concerning management, performance and control is handled by the senior staff level that belong to the management cadre in the organizations. A judgmental or non-statistical sampling technique was adopted in this study. This is because some selected banks may not cooperate in filling the questionnaire as expected. The factor considered by the researcher in the judgmental approach is the willingness of the branch manager to influence the management staff to fill the questionnaires without them being biased. Data analysis was done descriptively as well as empirically using regression model. From the model specification, $y = a + bx$. But from the objective, fraud management (FM) of the selected banks represent y while x represent the independent variable (BVN). Substituting these in the above equation, we have $FM = a + b \text{ BVN}$ (equation 2). Therefore, equation 2 was used in the regression analysis.

RESULTS AND DISCUSSION

Descriptive Analysis for the Selected Banks

Table 1: Mean Summary of Rated Responses on Effectiveness of BVN in Curbing Identity Theft and Safety of Depositors' Funds in the studied banks.

SN	ITEMS	SA(5)	A(4)	D(3)	SD(2)	U(1)	TOTAL	MEAN	REMARK
1	BVN prevents the occurrences of identity fraud in Nigerian commercial banks.	27 (135)	8 (32)	-	-	-	35 (167)	4.77	A
2	BVN limits the level of impersonation in commercial bank	28 (140)	7 (28)	-	-	-	35 (168)	4.80	A
3	BVN restrains fraudsters from opening accounts with personal information of other clients and issuing cheques on such account.	17 (85)	10 (40)	4 (12)	4 (8)	-	35 (145)	4.14	A

SN	ITEMS	SA(5)	A(4)	D(3)	SD(2)	U(1)	TOTAL	MEAN	REMARK
4	BVN also prevents imposters from having access to the accounts of dead clients	25 (125)	9 (36)	-	1 (2)	-	35 (163)	4.66	A
5	BVN limits fraudsters from opening credit card account using name and date of birth of reputed individuals to enable them run up charges without payments.	20 (100)	12 (48)	2 (6)	-	1 (1)	35 (155)	4.43	A
6	BVN prevents fraudsters from changing phone number, the email address and other relevant details relating to a customer's account and run transactions on his behalf.	18 (90)	13 (52)	1 (3)	3 (3)	-	35 (148)	4.23	A
7	BVN protects identity of bank customers before, during and after online and mobile transactions.	16 (80)	9 (36)	5 (15)	4 (8)	1 (1)	35 (140)	4.00	A
8	BVN equally reduces the involvement of bank staff in identity fraud	17 (85)	16 (64)	1 (3)	1 (2)	-	35 (154)	4.40	A
9	BVN reduces the rate at which foreign exchange regulations are breached through impersonation.	11 (55)	17 (68)	2 (6)	4 (8)	1 (1)	35 (138)	3.94	A
10	BVN disallows banks from exploiting the information they have in blackmailing customers with whom they have disagreements.	6 (30)	15 (60)	3 (9)	7 (14)	4 (4)	35 (117)	3.34	A
11	BVN ensures adequate security of the mobilized savings from depositors.	11 (55)	19 (76)	3 (9)	1 (2)	1 (1)	35 (143)	4.09	A
12	BVN is an effective internal control measure for proper management of depositors' fund.	14 (70)	17 (68)	-	3 (6)	1 (1)	35 (145)	4.14	A
13	BVN secures customers' financial details (like the total amount in a client's account) before, during and after every banking transaction.	19 (95)	14 (56)	-	1 (2)	1 (1)	35 (154)	4.40	A
14	BVN tracks customers' financial transactions across banks to ensure safety of funds	16 (80)	13 (52)	2 (6)	2 (4)	2 (2)	35 (144)	4.11	A
15	BVN also reduces the amount lost by commercial banks to cybercriminals.	17 (85)	12 (48)	3 (9)	3 (6)	-	35 (148)	4.23	A
16	The amount lost as a result of corporate fraud in commercial banks also decreased since the adoption of BVN	19 (95)	13 (52)	2 (6)	1 (2)	-	35 (155)	4.43	A
17	BVN identifies and blacklists fraudulent loan account accounts.	17 (85)	14 (56)	1 (3)	1 (2)	2 (2)	35 (148)	4.23	A
18	BVN also blacklists loan defaulters and stops them from moving from one bank to another to obtain new credit.	24 (120)	9 (36)	-	1 (2)	1 (1)	35 (159)	4.54	A
19	BVN enhances the liquidity position of banks commercial banks due to adequate management of	8 (40)	10 (40)	6 (18)	6 (12)	5 (5)	35 (115)	3.29	A

SN	ITEMS	SA(5)	A(4)	D(3)	SD(2)	U(1)	TOTAL	MEAN	REMARK
	depositors funds								
20	BVN also increases the level of financial stability in Nigeria banking sector.	14 (70)	12 (48)	1 (3)	5 (10)	3 (3)	35 (134)	3.83	A
	Total	344 (1720)	249 (996)	36 (108)	48 (96)	23 (23)	35 (2943)	84.09	
	Grand Mean	86.00	49.80	5.40	4.80	1.15	147.15	4.20	A

Source: Computation from survey data

A** is Accept

R** is Reject

Test of Hypothesis

H₀₁: BVN is not effective in curbing identity theft and safety of depositors' funds in the selected Nigerian commercial banks.

H_{a1}: BVN is effective in curbing identity theft and safety of depositors' funds in the selected Nigerian commercial banks

Decision Rule: Reject H₀ if P-value < 0.05; otherwise accept.

Table 2: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.136 ^a	.018	.011	.42844

a. Predictors: (Constant), effectiveness of BVN

b. Dependent Variable: Level of identity theft and safety of depositors fund

Source: SPSS Version 20.00

Table 3: ANOVA^b

Model	Sum of Squares	Df	Mean Square	F	Sig.
1					
Regression	.114	1	.114	.620	.000 ^b
Residual	6.057	33	.184		
Total	6.171	34			

a. Dependent Variable: Level of identity theft and safety of depositors fund

b. Predictors: (Constant), effectiveness of BVN

Source: SPSS Version 20.00

Table 4: Coefficients^a

Model	Unstandardized Coefficients		Standardized Coefficient	t-statistics	Sig.
	B	Std. Error	B		
(Constant)	0.091	0.115		0.787	0.000
Bank Verification Number	1.107	.171	.136	6.491	0.000

a. Dependent Variable: Level of identity theft and safety of depositors fund

Source; SPSS version 20.0

In the descriptive analysis, the researchers set a standard mean point of 3.0 out of the 5 mean points. A mean score of 3.0 and above on a five (5) point likert scale is considered accepted while a mean score that is less than 3.0 is considered not accepted or rejected. The result of the descriptive analysis shows that the predictor variable (Bank Verification number) has significant positive effect on the dependent variables (Fraud Management) since the grand mean score of 4.20 is above the standard mean point of 3.0. From the regression analysis, the R-value is 0.136^a which implies that there is a weak positive relationship at 13.6% between the dependent and independent variables. More so, the R-square value shows that 1.80% variation in level of identity theft and safety of depositors' fund is explained in the model. In addition, since the coefficient of the independent variable is 1.107, it therefore implies that BVN secures the deposits and personal

information of bank customers by 110.7%. Furthermore, the p-value is 0.000 and the standard p-value is 0.05 which shows 95% assurance of the research leaving 5% for uncertainty. As such, we reject the null hypothesis and accept the alternative hypothesis and conclude that BVN is effective in curbing identity theft and safety of depositors' funds in the selected Nigerian commercial banks.

These findings give credence to the study of Craven and Eloff (2012) who hold that out of all the fraud that occur in micro finance lending industry in South Africa, 20% is conducted using illegitimate ID book, and 30% is conducted through impersonation. The study also corroborates with the submission of Imuetinya Bernadette (2010) and Poee and Labuschaque who claim that biometric authentication improves identity and information security. It is equally supported by the study of Hosseini and Mohammed (2012) which shows that biometric authentication is a perfect solution to defeat financial fraud and ensure adequate security of depositors fund in the banking industry. All these reinforce the fact that BVN is effective in curbing identity theft and safety of depositors' funds in Nigerian commercial banks.

CONCLUSION

The current authentication methods in Nigerian banking industry (such as passwords, PINs, and tokens) are not perfect solutions and they don't offer adequate level of identity security. As such, the necessity for a more stronger and reliable authentication method such as biometric is obvious. The introduction of BVN as a strong biometric authentication technique is an identity security strategy to mitigate frauds and other financial malpractices and also ensure high level of financial security in Nigeria commercial banks. In line with the submission of other researchers, the rate of identity fraud in Nigerian commercial banks since 2014 till date tends to be low due to the effectiveness of bank verification number that has made it practically impossible for fraudster to impersonate a bank client and have access to his personal bank information. Finally, this study has established from the descriptive and inferential analysis of opinion of employees of selected banks in Ebonyi state, that the adoption of biometric system through BVN scheme has significant effect on fraud management of selected Nigerian commercial banks.

RECOMMENDATION

Based on the descriptive and empirical analysis, this study recommends that Nigerian commercial banks should extend biometric authentication systems to all of their operations like internet banking, mobile banking, ATM banking and Point of Sales (POS), etc. this is because biometric system increases security of depositors fund and other personal information of bank clients as well as prevents financial frauds in banking firms.

REFERENCES

- [1] Adewale, A. A., Ibidumi, A.S. and Badepo, J.O. (2014). Biometric Enabled E-Banking in Nigeria. Management and Customers Perspective. *Journal of Information and Knowledge Management*, 4(11).
- [2] Adeyemo, K A. (2012), Fraud in Nigeria Banks: Nature, Deep Seated Causes, Aftermaths and Probable Remedies. *Mediterranea Journal of Social Sciences*, 3(2), 279-289.
- [3] Ajzen, I., and Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behavior. *Englewood Cliffs, NJ: Prentice-Hall*.
- [4] Ajzen, I. (1991). The Theory of Planned Behavior: Organizational Behavior and Human Decision Processes, p179-211.
- [5] Akinnwesi, B.A., Uzoka, F.M.E., Okwundu, O.S., & Fasholo, G. (2016). Exploring Biometric Technology Adoption in a Developing Country Context Using the Modified UTAUT. *International Journal of Business Information System*, 23(4), 482-521.
- [6] Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K. and Senior, A. W. (2003), "Guide to Biometrics", Springer, New York.
- [7] Bamidele, O. (2015). Bank verification Number as an antidote to bank fraud in Nigeria. Retrieved from <https://www.newsbeatportal.com/bank-verification-number-as-antidote-to-bank-fraud-in-Nigeria/?dx-switcher=true>
- [8] Craven & Eloff, M. (2015). Biometric as an Agent to Reduce Fraud in The Micro Lending Industry in South Africa. University Of South Africa 0003.
- [9] Capoor, S. (2006), "Biometrics as a Convenience", Security: For Buyers of Products, Systems & Services, 43(12), 48-50.
- [10] Central Bank of Nigeria Act (2007). Federal Republic of Nigeria Official Gazette, 55(94)
- [11] Central Bank of Nigeria Manual (2009). Anti-Money Laundering/Combating Financing of Terrorism Compliance for Banks and Other Financial Institution in Nigeria.
- [12] Chima, A. (2014). Nigeria: Banks lose N159billions to cybercrime. Retrieved from <https://allafrica.com/stories/201406230436.html>
- [13] Conroy, J. (2017). Moving Beyond the Password: Consumers' Views On Authentication. *Aite Group*. Retrieved From [Http://Www.Aitegroup.Com/Report/Moving-Beyond-Password-Consumers%E2%80%99-Views-Authentication](http://www.aitegroup.com/Report/Moving-Beyond-Password-Consumers%E2%80%99-Views-Authentication).
- [14] Davis, F., Bagozzi, R., and Warshaw, R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*. 35(1) 982-1003.
- [15] Davis, F. D. (1986). A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results. Doctoral Dissertation.

Cambridge, MA: *MIT Sloan School of Management*.

- [16] Ehi, E. E. (2015). A Critical Analysis of the Bank Verification Number Project Introduced By The Central Bank Nigeria. *DSC Publication Ltd*. Retrieved from www.researchgate.com.
http://www.cgap.org/gm/document-1.9.47443/FN_64_Rev.pdf
- [17] Hauser, J. R., and Shugan, S.M. (1980). Intensity Measures of Consumer Preference. *Operation Research*, 28(2), 278-320.
- [18] Hosseini, SS., Mohammadi, S., 2012. Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System. *Journal of Basic and Applied Scientific Research*, 2(9), 9152-9160.
- [19] Imuetinyan, B.I. (2010). Towards Implementing an Efficient Biometric Authentication Framework for Nigeria customer Banking Systems. *Information Manager*, 10(2).
- [20] Idolor, E. J. (2012), Bank Fraud in Nigeria: Underlying Causes, Effects and Possible Remedies, *African Journal of Accounting, Economics, Finance and Banking Research*, 6(6),62.
- [21] James E (2014). Nigerian Banks Lose N5.76bn to fraud in 2013-ndic. Retrieved from <http://sweetcrudereports.com/2014/12/03/nigeria-banks-lose-n5-76bn-to-fraud-in-2013-ndic/>
- [22] Jain, A. K. (2004) Biometric recognition: How do I know who you are? *Signal Processing and Communications Applications Conference. Proceedings of the IEEE 12th*.Kusadasi, Turkey. p3-5.
- [23] Juniper Research (2018) Mobile banking users to exceed 1.75 billion by 2019. Retrieved from <https://www.juniperresearch.com/press-release/digital-banking-pr1>
- [24] Ogunleye, G. O., Fashoto, S. G., Andile M., and Ogunde, A.O. (2017). Development of an Online Bank Verification Number System Using Linear Congruential Algorithm. *Information Technology Journal*, doi=itj.2017.62.70
- [25] Orji, V, O. (2015). Knowledge Management System: Issues, Chalaenges, and Benefits. *Communication of the Association for Internation System*, 1(7).
- [26] Pooe, A.& Labucshague, L. (2011). Factors Impacting on the Adoption of Biometric Technology by South African Banks: An Empirical Investigation. *South Africa Business Review*.15(1)
- [27] SitalakshimiVenkatraman, IndikaDelpachita, (2008) "Biometric in banking security: a case study", *Information management & Computer Security*, 16(4)415-430,
<https://doi.org/101108/09685220810908813>.
- [28] Venkatesh, M.G., Morris, G.B., Davis, F.D.(2003). User Acceptance of Information Technology: Toward a Unified View, *MIS Quart.* 27 (3). 425–478.