AGJ
ARABIAN GROUP OF JOURNALS

# Social Development

NG-Journal of Social Development, VOL. 6, No. 1, February 2017

Journal homepage: www.arabianjbmr.com/NGJSD_index.php

NGJSD

## IMPACT OF BIOMETRIC TECHNOLOGY ON DEPOSIT MONEY BANKs PERFORMANCE IN NIGERIA

**Akpokerere Othuke Emmanuel**
**Oboro Oghenero Godday**
*Department of Banking and Finance, Delta State Polytechnic, Ozoro*

**Abstract**

*This study investigates impact of biometric technology on deposit money banks performance in Nigeria with special emphasis on eight selected banks in Asaba, Delta State. The specific objectives of the study was to determine the impact of biometric on banking services and ways fraud can be reduce through biometric technology. Analysis of variance was the statistical technique used for the analysis while data were presented by use of tables, percentages and means. The study revealed that biometric technology has significant impact on banking services, this could be due to the fact that the Central Bank requires banks to increase their deployment of new technologies to protect customers' interest and loyalty. We conclude that banks should adopt adequate security tool like biometric technology that will help them to provide high level of security for every of their transactions to gain customers' trust and avoid regulatory fines and recommend that banks should develop more customized software that can record relevant information in all channels of banking so that banks can establish whether unauthorized transactions has taken place or not.*

***Keywords**: Biometric technology, Deposit money banks, performance and analysis of variance*

### Introduction

Biometric security is the science of authenticating physical characteristics such as fingerprints, eyes and hands to identify and authenticate a person and the products used in this system include fingerprint readers and retinal scanners. Gunaji and Pranav (2010), biometric technologies offers higher security levels by simply ensuring that the authorized individual is physical present to gain access. When you are considering biometric security, you want to have physical characteristics that are constant and do not change over time and are also difficult to fake or change on purpose. Biometric identity verification and authentication provides more and more monetary security and protection from identity theft (Ahmed and Mohamed, 2013). Password and PIN numbers are the major target to be stolen or revealed and afterward exploited by people with criminal mentality over the internet and also at banking and business networks. According to Batiz-Lazor et al (2005), switching from conventional security procedures to biometric physical access control eliminates the need for multi-password system and different processes and integrates entire access into one touch of the finger, scan of the eyes, etc.

Biometrics technology can be easily integrated with the financial organizations such as banks, ATM machines can be used at retail locations with smart cards, credit cards and debit cards, and anywhere you may make a financial transactions. It will act on its own or in conjunction with your PIN to securely identify you as the owner of the card and the person who has access to the money being exchanged. If a database of known person has been developed, then it is possible to answer the question of the person identify 'who are you?' The biometric of any unknown person can be compared against the database in a search. Their identity can be determine if their biometric has been entered onto the database on a previous occasion; this is much quicker than a manual system. There should be high quality data needed if the database searches are to give accurate and instant results (Ahmed and Mohamed, 2013).

A better security measure will be through biometric technology to validate access to the online applications. Since biometric technology utilizes certain physical and behavioural traits that are unique

to an individual to identify and verify a person, it may therefore provide a better method for identification as compared to other security measures. Since a biometric device uses a unique biological trait to distinguish an individual, it is very difficult and often impossible for the identifier to be lost, stolen, duplicated, or given away (Chan 2008). This benefit makes biometric technology a very attractive option for banks, companies and government agencies that want to adopt new security technology for their online applications.

**Statement of the problem**

The sharp rise in sophisticated bank fraud and the increase in identify theft throughout banking systems has increased demand for a more secure method to identify customers that do not rely on something they secure have or something they know, but rather who they are. In addition, a significant increase in digital, online and mobile banking services has pushed secure customer authentication to the priority list for most banks and financial institutions, Gee and Thamaralse (2013). Traditional methods of customers authentication such as password, PINs, and tokens are now obsolete, easy to forge, and cannot protect consumer information from being compromised. Lack of security technologies and protection in identity theft and weak authentication methods often causes devastating financial and transactional data breaches, lending to significant financial losses to customers and large regulatory fines levied on financial organizations. Almost every day, we read reports on how bad the security is in the internet. In computer security world, it is nearly impossible to keep up with the flood of detail about new viruses, worms, spam, spyware, or other attacks against computers on the network. A malicious software termed spyware is becoming more common. Spyware is the name of a broad class of software that collects information about activity on your computer and reports to someone on the internet (Chan 2008). In relation to customer's satisfaction, most customers complain of time wasted in banks, mostly when there is network failure due to linkage problem they encountered through internet banking. This aside, the banks have since 2000 been introducing payment cards in form of Automated Teller Machine (ATM) cards, but usage has been very low due to lack of interconnectivity and insecurity. To resolve some of these problems, biometric technology comes to play.

**Objectives of the study**

The broad objective of the study is impact of biometric technology on Deposit Money Banks. The specific objectives are as follows:

1. To determine the impact of biometric technology on banking services.
2. To examine the ways fraud can be reduce through biometric technology.

Research questions

The following research questions were formulated to guide the study:

1. To what extent do biometric technology impact on banking services?
2. To what magnitude can fraud be reduce through biometric technology?

**Research hypotheses**

This study is guided by the following hypotheses stated in the null form:

$H_{01}$: Biometric technology has no significant impact on banking services.

$H_{02}$: Fraud cannot be significantly reduce through application of biometric technology in banking services.

## LITERATURE REVIEW

## CONCEPTUAL FRAMEWORK

**Meaning of biometric identification**

The term "biometric" is derived from the Greek words "bio" (life) and "metrics" (to measure). Biometric identification exploits the universally recognized fact that certain physiological or behavioural characteristics reliably distinguish one person from another (Chan, 2008). Biometrics refers to automatic system that uses measurable physiological characteristics or behavioural traits to recognize the identity or authenticate the claimed identify of an individual. Biometric systems based on single source of information are called Unimodal systems. Jain et al (2006) provided several definitions of biometrics which include:

- Biometrics = identification/verification of persons based on the unique physiological or behavioural features of humans.

- Biometrics is the measurement and matching of biological characteristics such as finger print images, hand geometry, facial recognition, etc.
- Biometrics is strongly linked to a stored identity to the physical person.

In spite of the various definitions, it can be seen that the science of biometrics is based on the fact that no two people are the same and this has a significant influence on its reliability and success factor. According to Ihejiahi (2009), there are three ways to establish the identify of a person are something know " (e.g., password, PIN) which provides first level of security and something you carry" e.g., ID card, smart card and something you are (biometrics), these provide second level of security. In smart card, the fingerprint templates are encoded into a smart card memory, to identify a person, his/her fingerprints are compared against the digital templates stored in the card memory. Identify management system is to find the individual's identify.

Traditional methods of establishing a person's identify include knowledge-based and token-based mechanisms which can be easily lost, shared or stolen. To overcome all these problems biometrics was introduced. Physical biometric is a static biometrics and the data is derived from the measurement of an action performed by an individual. It includes fingerprint, iris, retina, hand geometry, palm print, face recognition, DNA and vascular pattern recognition.

- Fingerprint- Analyzing fingertip patterns.
- Facial Recognition- Measuring facial characteristics.
- Hand Geometry- Measuring the shape of the hand.
- Iris Recognition- Analyzing features of coloured ring of the eye.
- Vascular Patterns- Analyzing vein patterns.
- Retinal Scan- Analyzing blood vessels in the eye.
- Bertillon age- Measuring body lengths (no longer used).

Behavioural biometrics is a dynamic biometric and the data is derived from the measurement of an action performed by an individual and the parameter considered over here is time; the measures action has a beginning, middle and end. It includes signature, keystroke, handwriting, voice recognition and Gait.

- Speaker Recognition- Analyzing vocal behavior.
- Signature- Analyzing signature dynamics.
- Keystroke- Measuring the time spacing of typed words.

Soft biometrics also known as chemical biometrics is a human characteristics that provide some information about the individual. It includes height, weight and colour of hair (Gee and Thamaraiselvi, 2013). Automated biometrics systems have only become available over the last few decades, due to significant advances in the field of computer processing.

Application of biometrics in internet banking for authentication

Utilizing biometrics for internet banking is becoming convenient and considerable more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links the event to a particular individual (a password or taken may be used by someone other than the authorized user). It is convenient (nothing to carry or remember). Accurate (it provides for positive authentication), and also can be audit trail and is becoming socially acceptable inexpensive, Gunaji and Pranav (2010).

Benefits of using biometrics in banking

1. Protecting information: Biometric technology provides the strongest method of authentication that protects banking information from being compromised by unauthorized personnel.
2. Fast and accurate branch banking: Biometric technology provides fast and accurate identification for the banking industry. Customers can be quickly authenticated in mere seconds through a fast biometric scan.
3. Protection against insider fraud: Biometric identification of employees performing transactions on the bank end is a crucial step to ensuring identity protection and reducing fraud. Biometric in banking will help financial institutions to prevent insider fraud by establishing secure employee authentication, accountability and concrete audit trail of each transaction.
4. Secure online banking: Over the past years the banking sector has been suffering from massive online service cyber-attacks. In most of these cases customers lose their money from the negative effects of identity theft. Biometrics in banking helps the bank to protect customer identities when using banking services.

5. ATMs with Biometrics: Biometrics in banking for ATMs authentication brings outstanding benefits to both customers and banks. This system now gives customers flexibility to make transactions without bringing bank cards. Banks avoid the costs and liabilities of customer problems due to lost or stolen bank cards.
6. Audit Trails: Banks can easily track and monitor employee and customer activity in the system to create concrete audit with biometric technology solutions.
7. Fast, Secure and Accurate Customer Care Service: The banking sector is always in need of tighter security solutions to provide improved and more secure customer care service over the phone and internet. A biometric voice recognition system for example provides a secure and flexible solution to verify and customer executing transactions outside of a brick and mortar environment.

## THEORETCAL REVIEW

Models and theories on adoption of new technologies

There are various theories and models used in adoption of new technologies such as theories of reasoned action by Fishbein and Ajzen, 1975, the theory of planned behavior Ajzen (1983), technology acceptance model by Adams and Sasse (1992); Davis, Bagozi and Warshaw (1989) and many others theories. However, this study adopted technology acceptance model.

The technology acceptance model developed by Davis et al (1989), states that beliefs influence attitudes about information technology, which lead to intentions and subsequently behaviours of actual technology usage. Davis (1989) has shown that perceived usefulness and perceived ease of the use of the technology influenced the beliefs that leads to system usage. Based on TAM, the better is the individual interest towards the new technology and the higher the intention to adopt it.

Many studies have use technology acceptance model to evaluate user adoption of various information technologies like e-commerce, e-government, internet banking, mobile banking, e-learning, open source software, mobile credit card and internet tax-filing system

## METHODOLOGY

The researchers used descriptive survey method in the study as this gives greater room to study the subject matter and ensure that inferences can be made about the behavior of the population examined in the study. All the deposit money banks that operate in Asaba and all customers made-up the population of the study. However, the researchers sample only eight banks which includes; First bank PLC, Diamond bank PLC, Union bank PLC, Unity Bank PLC, Access bank PLC, Eco bank PLC, Zenith bank PLC, Sterling bank PLC and customers randomly selected. Structures questionnaire was designed and administered on 125 bank staff respondents randomly. The staff included top and middle level management staff while 81 customers were also randomly selected.

The questionnaires were divided into two section. Section one sought information from bank staff while section two sought information from bank customers. A 5 point scale was used to measure the level of agreement or disagreement by the respondents. The response format was: SA= Strongly Agree, A= Agree, N= Neutral, SD= Strongly Disagree and D= Disagree.

The method used for presentation of data includes the use of tables, percentages and means. A statistical analysis known as analysis of variance (ANOVA) was used for the study. Analysis of variance (ANOVA) is a statistical technique used for portioning the variation in an observed data into its different sources.

## DATA PRESENTATION AND ANALYSIS

### Presentation of data

This section presents and interprets data regarding impact of biometric technology in the deposit money banks (DMBs) in Nigeria. The descriptive statistics and the homogeneity of variance test were presented in order to ensure that our date set and variables are in consonance with the existing assumptions. The above measure ensured that our analysis of variance test results are reliable and non-spurious.

### Test of hypotheses

This section tests the hypotheses stated in chapter one. Three steps were utilized in interpreting ANOVA results. The steps involved, (i) presenting and analyzing the preliminary test results (the descriptive statistics and the Homogeneity of variance tests), (ii) restating the hypotheses in Null and Alternate

forms, (iii) presentation and interpreting the ANOVA results and, (iv) using the decision criteria to accept or reject the null/alternate hypotheses.

Testing of hypothesis one

Step one: presentation of preliminary tests

**Table 1: descriptive statistics**

| | N | mean | Std. deviation | Std. Error | 95% confidence interval for mean | | minimum | maximum |
|---|---|---|---|---|---|---|---|---|
| | | | | | Lower bound | Upper bound | | |
| Staff | 125 | 2.1280 | 1.15686 | .10347 | 1.9232 | 2.3328 | 1.00 | 5.00 |
| Customers | 81 | 1.7407 | 1.26271 | .14030 | 1.4615 | 2.0199 | 1.00 | 5.00 |
| Total | 206 | 1.9757 | 1.21149 | .08441 | 1.8093 | 2.1421 | 1.00 | 5.00 |

Source: researchers SPSS Result.

Table 1 shows that our 'N' is correct and in agreement with the responses from each group-staff (125) and customers (81) with a total of 206 as reflected on the questionnaire returned. The mean and the standard deviation are on the same scale, which indicates that the distribution is symmetrical. It can also be observed that the confidence interval is 95%, which is quite high and desirable.

**Table 2: Test of homogeneity of variances**

| Levene statistic | Df 1 | df 2 | Sig. |
|---|---|---|---|
| 2.663 | 1 | 204 | 104 |

Source: researchers SPSS result

The assumption of variance is that the variance or our variable are equal at every point. The null hypothesis is that the variance across the levels are the same. Accept the null hypothesis when the p value is greater than 5% critical value, and we reject when the p value is less than 5%. From table 2, the assumption of homogeneity of variance was tested and found tenable using levene's Test, F(2, 204) = p = 0.104. Since the p value (0.104) is greater than 0.05 we come to the conclusion that our variances are homogenous.

Step two: Restating the hypothesis in Null and Alternate forms

$H_0$: Biometric technology has no significant impact on banking services.

Step three: presentation and interpretation of ANOVA Results

**Table 3: ANOVA**

| | Sum of Squares | Df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 7.371 | 1 | 7.371 | 5.123 | .025 |
| Within Groups | 293.508 | 204 | 1.439 | | |
| total | 300.879 | 205 | | | |

Source: researchers SPSS Results.

Table 4.3 presents the analysis of variance result of hypothesis one. The mean squares for variances between groups and within groups are 7.371 and 1.439 respectively. The F-statistics is 5.123, while the significance value, or p value is 0.025 < 0.05. Since the F value is non-negative and the significance value is less than 5% (0.05) critical value, we infer that our result is positive and highly significant.

Step four: decision Rule

Here we use the decision criteria to accept or reject the null/alternate hypotheses. If the p value is greater than 5%, we accept the null hypothesis and reject the alternate hypothesis. Conversely, if the p value is less than 5%, we reject the null hypothesis and accept the alternate hypothesis. As revealed in our AVANO table, the p value 0.025 is less than 0.05 critical value. We therefore reject the null hypothesis and accept the alternate hypothesis that biometric technology has significant impact on banking services.

**Test of hypothesis two**

Step one: presentation of preliminary Tests

**Table 4: Descriptive Statistics**

| | N | mean | Std. deviation | Std. Error | 95% confidence interval for mean | | minimum | maximum |
|---|---|---|---|---|---|---|---|---|
| | | | | | Lower bound | Upper bound | | |
| Staff | 121 | 1.7438 | 1.08420 | .09856 | 1.5487 | 1.9390 | 1.00 | 5.00 |
| Customers | 85 | 1.4471 | .80926 | .08778 | 1.2725 | 1.6216 | 1.00 | 4.00 |
| Total | 206 | 1.6214 | .98888 | .06890 | 1.4855 | 1.7572 | 1.00 | 5.00 |

Source: Researchers SPSS Results

Table 4 shows that our 'N' is correct and in agreement with the responses from each group-staff and customers, with 121 and 85 respondents respectively. The mean and the standard deviation are on the same scale, which indicates that the distribution is symmetrical. It can also be observed that the confidence interval is 95%, which is quiet high and desirable.

**Table 5: Test of homogeneity of variances**

| Levene statistic | df 1 | df 2 | Sig. |
|---|---|---|---|
| 3.606 | 1 | 204 | .039 |

Source: researchers SPSS result

The assumption of variance is that the variances or our variable are equal at every point. The null hypothesis is that the variances across the levels are the same. We accept the null hypothesis when p value is greater than 5% critical value, and we reject when the p value is less than 5%. From table 5, the assumption of homogeneity of variance was tested and found tenable using Levene's Test, F(2, 204) = p = 0.079. Since the p value (0.079) is greater than 0.05 we come to the conclusion that our variances are homogenous.

Step two: Restating the hypothesis in Null and Alternate forms

$H_1$: Fraud cannot be significantly reduced through application of biometric technology in banking services.

**Table 6: ANOVA**

| | Sum of Squares | Df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 4.396 | 1 | 4.396 | 4.574 | .034 |
| Within Groups | 196.070 | 204 | .961 | | |
| total | 200.466 | 205 | | | |

Source: researchers SPSS Results.

Table 6 presents ANOVA result of hypothesis two. The mean squares for variances between groups and within groups are 4.396 and 0.961 respectively. The F-statistic is 4.574, while the significance value or p value is 0.034 <0.05. Since the F value is positive and the significance value is less than 5% (0.05) critical value, we infer that our result is positively and highly significant.

Step four: decision Rule

Here we use the decision criteria to accept or reject the null/alternate hypotheses. If the p value is greater than 5%, we accept the null hypothesis and reject the alternate hypothesis. Conversely, if the p value is less than 5%, we reject the null hypothesis and accept the alternate hypothesis. As revealed in our AVANO table, the p value 0.034 is less than 0.05 critical value. We therefore reject the null hypothesis and accept the alternate hypothesis that fraud and identity theft can be significantly reduced through application of biometric technology in banking services.

## SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

### Summary of findings

Testing hypothesis one, it was found that the p value 0.025 is less than 0.05 critical value, then we therefore reject the null hypothesis and accept the alternate hypothesis that biometric technology has significant impact on banking services. This could be due to the fact that the Central Bank of Nigeria requires banks to increase their deployment of new technologies to protect customers' interest and loyalty.

Testing hypothesis two, it was found out that the p value 0.034 is less than 0.05 critical value and so the null hypothesis was rejected and the alternate hypothesis accepted and therefore we conclude that fraud and identity theft can be significantly reduced though deployment of biometric technology in banking system. This implies that the size of crime in online banking or internet banking can be reduced through deployment of biometric technology. This could be due to tremendous growth and development of technological advancement that has been a driving force in the banking system. Banks and financial institutions need to come forward to adopt adequate security tools like biometric technology in banking that can empower them to provide the highest level of security for every transaction to gain customer trust and avoid regulatory fines.

### Conclusion

Banks and financial institutions play major roles in the economic development of a country and the success of banks and financial institutions are largely dependent on customers trust and loyalty. Identify fraudulent activities in banking transaction have affected the industry's growth. Banks need to come forward to adopt adequate security tools like biometric technology in banking that can empower them to provide the highest level of security for every transaction to gain customer trust and avoid regulatory fines. Biometric technology, integrated with the existing traditional security system will empower banks to deploy the highest level of authentication security possible. Both customer and management support the notion that biometric technology will reduce and curtail frauds activities, enhance overall customer satisfaction and achieve more effective relationship between customers and their bankers.

Recommendations of the study

The following recommendations are made based on the findings of the study:

1. Banks should develop more customized software that can records relevant information in all channels of banking so that banks can establish whether unauthorized transactions has taken place or not.
2. Banks should hold firm the laws on fraudsters and scammers so as to boost economic of the nation.
3. Banking managers and government should properly adopt strategy that will encourage businessmen and general public in using all channels of banking which will improve effectiveness and efficient of the banking sector.
4. There is the need to educate customers extensively on the use of electronic services such as internet banking, SMS (mobile) banking and point of sale banking services which are not well patronized.

### References

Adams, A. and Sasse, M. (1999). Users are not the enemy. *Communication of the ACM 42,no 12.*

Ahmed T.S and Mohammed M (2013). Study of Biometrics Solution to curb fraud in ATM Transaction. *IJASCSE, Vol.s, Theme based issued 3, pp 1-6*

Batiz-Lazor, B. and Barrie, A. (2005). The business and technology history of automated teller machines in the UK, 1967-2005, A Primer Conference Abstracts, 16-17th June. *Queen Mary, University of London.*

Chan K.L, (2008). Adoption of biometric technology in online application, research report.

Davis, F.D., Bagozzi, R. and Warshaw, (1989). User acceptance of computer technology. *A comparison of two theoretical models, management science 35, no. 8, 982-1003.*

Fishbein, M. and Ajzen, I. (1975). Belief attitude intention and behavior. *An introduction to theory and research Addison Wesley, reading, MA.*

Gee I.T and Thamaralse K (2013). Enhancing the security of biometrics in ATM, International Journal of Scientific and Engineering Research. *Volume 4; issue 4, April 2013 ISSN 2229-5518.*

Gunajit S and Pranav K.S (2010). Internet banking; risk analysis and application of biometric technology for authentication. *International Journal of Pure and Applied Sciences and Technology ISSN 2229-6107.*

Ihejiahi R 2009. How to fight ATM fraud online. *Nigeria Daily News, June 21, 18.*

Jain A.K, Bolle R and Pankanti S. (2006). Introduction to biometric. The Kluwer international series in engineering and computer science. *Kluwer Academic Publisher, New York.*

Jain A.K, Ross. A and Pankanti S. (2006). Biometrics, a tool for information security. *IEEE Transaction on information Forensics and Security 1(2), 2006.*

Muhammed, A.K. (2010). An empirical study of Automated Teller Machine service quality and customer satisfaction in Pakistani banks. *European Journal of Social Sciences, vol. 13 no.3, pp. 333-344.*