**DESIGN AND IMPLEMENTATION OF AN ONLINE BANK VERIFICATION NUMBER (BVN) SYSTEM**

**ABSTRACT**

The Bank Verification Number (BVN) became imperative following the increasing incidence of compromise on conventional security systems such as password and Personal Identification Number (PIN) of customers. The BVN involves identifying an individual based on physiological or behavioral attributes, such as fingerprint, signatures and others. The customers unique BVN is accepted as a means of identification across all banks system.On the basis of introducing the concepts of Bank Verification Number system, this project work illustrates the role that the BVN plays in Nigerian banks.This research work also analyses the existing mode of operation in the banking industry including the need to implement our newly designed Online Bank Verification Number system using PHP as the programming language.

**CHAPTER ONE**

**INTRODUCTION**

Faced with the problem of insecurity on customer accounts, the Central Bank of Nigeria (CBN) on February, 2014 initiated a compulsory bank verification number exercise which provides account holders with a unique number that enables the account holder to have a single identity in the banking system aimed at protecting bank customers from identity theft and other financial/economic crimes emanating in the banking sector of Nigeria (Orji, 2014) .

The Bank Verification Nlumber (BVN) is a bold step taken by the Central Bank of Nigeria, to strengthen security in the banking sector of Nigeria. One beauty of the BVN is that transactions will be safer once it is implemented fully. The BVN exercise aims at ensuring that bank transactions are safer and fraudulent transactions are minimized, if not totally eliminated. The campaign is on, but the public may not realize its importance until it closes in in the new extension deadline, October 2015.

BVN uses biometric technology to register customers in the banking sector. It records these physical features which are unique to individuals – fingerprints and the face. The record would be used to identify the person afterwards. Once a person’s biometrics have been recorded, and BVN issued the account would be accessed through BVN. The major objectives of the initiative are to protect bank customers, reduce fraud and strengthen the Nigerian banking system.

Biometric enrolment is helpful to people who cannot read and write. Their finger prints and pictures would serve the same purpose as signatures. Multiple account holders would be covered with a single registration in any of the banks where they have accounts.

BVN will help the banking system reduce situations where loan defaulters, for instance, move from one bank to the other and the banks extend new credits to them, without knowing their history.  Banks would be able to track transactions across all banks in Nigeria with more ease.

**1.2 STATEMENT OF THE PROBLEM**

Over the years, the banking sector of Nigeria has played the role of the intermediate body in regards to ensuring the smooth running of the economy and coordination other sectors involved in the circular flow of income in the Nigerian economy. However, growth in this sector has been reduced due to high cases of economic and financial crimes (Udenze, 2014). Fraud and money laundering have had adverse impacts on our national development and particularly on the financial system. They have caused damage to the reputation of the image of the country, loss of FDI, poor infrastructural devel­opment, dwindling confidence and distortions in our political as well as financial systems, among other things.

In view of these crises crimes perpetuated by cyber thieves, the mandatory bank verification number exercise embarked by various banks nationwide has also caused congestions in banking halls. Although the exercise commenced since February, 2014, the fire brigade approach of most Nigerians has warranted most bank halls to be filled to its maximum capacity. Queues in some banks even extended outside the banking hall. This development has caused confusion in some banking halls as other transactions are placed on hold due to inadequate staff to attend to clients or delayed indefinitely.

**1.3 RESEARCH OBJECTIVES**

The main objective of this paper is to design and implement a computerized Bank Verification Number System for Nigerians in the Diaspora and at home to use. Specific objectives of the study are:

1. To examine the benefits of adopting an online BVN system.
2. To identify the necessary structures need to run a successful online BVN system.
3. To identify challenges in the design and implementation of an online BVN system.
4. To design and implement and online BVN system.

**1.4 RESEARCH QUESTIONS**

1. What are the benefits of adopting an online BVN system?
2. What necessary structures are needed to run a successful online BVN system?
3. What challenges exist in the design and implementation of an online BVN system?

**1.5 SIGNIFICANCE OF THE STUDY**

The study will aid in reducing queues at banking halls and reducing identity theft if successfully implemented. Bank managers and other stakeholder in the banking industry of Nigeria can use this web application to restore confidence in the banking sector as more clients will be assured that their funds are safe, and the stress of queuing at banks will be totally eliminated.

The study will also serve as a guide to other student researchers who may want to conduct further research on the subject matter. Findings and recommendations from this system will aid in developing newer versions to serve optimally.

**1.6 DEFINITION OF TERMS**

**BVN:** Bank Verification Number

**CBN**: Central Bank of Nigeria

**Biometrics**: Biometrics refers to identification of an individual based on physiological attributes- fingerprint, voice, facial features etc.

**REFERENCES**

# Udenze, B. (2014). *BVN: CBN targets 80% fraud reduction in*

# *banking sector*. Obtainable at <http://sunnewsonline.com/new/bvn-cbn-targets-80-fraud-reduction-banking-sector/>

Orji, V, O. (2015).*Knowledge management systems: Issues,*

*challenges, and benefits*. Communications of the Association for Information Systems, 1(7).

**CHAPTER TWO**

**2.0 INTRODUCTION**

This chapter is concerned with the review of related literature, the contributions of other researchers is examined in this chapter. It looks at:

* The meaning of Bank Verification System (BVN)
* The importance of BVN
* Enrolment process
* NUBAN (Uniform Bank Account Number)
* Differences between BVN and NUBAN
* Conceptual Issues

**2.1 WHAT IS BANK VERIFICATION NUMBER(BVN)**

It is a scheme introduced by the Central Bank of Nigeria (CBN) to protect customer’s transactions and enhance confidence in banking. It involves capturing customer’s fingerprint and signature, among others, at their banks.

Due to the level of revolution that has taken place in the banking sector in Nigeria, banks have become completely Information Technology IT compliant in their business operations. But it is sad that fraudulent individuals have been having a field day as they have created a way of hacking into and manipulating the banks’ payment system to commit fraud. This is why the ongoing Bank Verification Number BVN project, initiated by the Central Bank of Nigeria CBN aimed at protecting bank customers and strengthening the banking system in a whole is, indeed, laudable and a right steps in the right direction.

Meanwhile, many Nigerians and bank customers have not realized the need to comply with the directive. It is either many of them do not understand the rationale behind the initiative or they are not even aware at all.

To be sure, the CBN’s BVN programme is an initiative where customers in the financial system get registered using biometric technology which involves the process of recording a person’s unique physical traits such as fingerprints and facial features. This record can then be used to correctly identify the person afterwards. Once these are properly captured, then the person is given a BVN PIN number.

More so, it is imperative to note that in the BVN programme, no two persons will have the same biometric information. As such, it will be easier for banks to check the features of a person doing a transaction against the record which the bank has captured thereby correctly identifying the owner of an account.

Fundamentally, it is meant to protect bank customers, reduce fraud and further strengthen the Nigerian banking system.  Recently, the Group managing Director/Chief Executive Officer of Fidelity Bank Plc, MrNnamdiOkonkwo in a statement, accentuates this fact as he emphatically stated that the BVN programme will be used to manage the credit score of bank customers. To this end, credit report from credit bureaus, would help lenders to determine who really qualifies for a loan as identities provided by the exercise would be matched against the information. As a matter of fact, this will help check credit worthiness of borrowers as the BVN initiative will provide a centralized customer biometric information system in the banking sector which will make it difficult for people who take multiple loans with no intension of repayment to operate. There is no doubt that the activities of such people are inimical to progress in the banking sector.  It must be understood that one of the beauties of the BVN initiative is that the PIN number obtained in the exercise is unified. In other words, the information generated on registration at one point, will automatically be linked to all the banks. So, one does not need to register in all the banks he operates an account in.

**2.2 THE IMPORTANCE OF BANK VERIFICATION NUMBER**

The [Central Bank of Nigeria](http://nairabrains.com/tag/central-bank-of-nigeria/) through the Banker’ Committee and in collaboration with all banks in Nigeria on February 14, 2014 launched a centralized biometric identification system for the banking industry tagged Bank Verification Number (BVN) which provides the following benefits to customers:

* Customers Bank Accounts are protected from unauthorized access
* It will address issues of identity theft, thus reduce exposure to fraud
* The BVN will enhance the Banking Industry chances of being able to fish out blacklisted customers
* This will improve speed of service and reduce queues in banking halls.
* Standardized efficiency of Banking operations
* It will make life and banking operations easy for bank customers as BVN is accepted as a means of identification across all banks in Nigeria (not peculiar to one Bank).
* It will enhance credit advancement to Bank customers

2.3 ENROLMENT PROCESS

The enrolment process is simple and easy. The best way of enrolling remains direct communication with one’s bank. Here are the reliable steps all bank customers must follow, about Bank Verification Number in order to achieve a seamless registration.

The enrollment process for acquiring your BVN is simple.

– Visit any branch of the bank you have an account with. Registration by proxy not acceptable.

– Collect and fill the BVN enrollment form with all personal data about you.

– Submit the completed form to a designated official at your bank, who would then transfer the information given into a computer data base.

– The official will take your photograph and finger prints.

– You will sign your signature that will be captured electronically into the data system.

– A small temporary registration acknowledgement slip will be issued to you, followed by an email or SMS conveying a similar information.

– A BVN identification card with a computer chip bearing your embedded personal information will be issued to you for collection at your designated bank branch.

– BVN registration exercise is mandatory for all individual customers.

– Registration must be completed on or before October 30, 2015.

– After deadline, you may not be able to do any financial transaction in any bank in the Nigerian banking system as you will require your fingerprint for authentication.

– BVN registration is for individual account holders for the meantime till further notice.

– Registration in one bank covers all accounts the individual might have in all other banks.

Once a person’s biometrics has been recorded, and BVN issued, the account would be accessed through BVN.

**2.4 NUBAN (Nigerian Uniform Bank Account Number)**

**2.4.1 WHAT IS NUBAN?**

NUBAN is an acronym for Nigerian Uniform Bank Account Number. NUBAN has great potentials to resolve the observed problems with electronic payments in Nigeria, as many of them are related to specification of wrong beneficiary account numbers. All Deposit Money Banks are advised to adopt this uniform algorithm to obtain the check digit component of NUBAN codes of their customer account numbers.

2.4.2 **TRANSITION**

Previously, different banks have used different account number formats for their customers. Some were less than or more than 10 digits.

While this diversity had its advantages, the disadvantages were greater as we are moving to the electronic payment era. The NUBAN code had been communicated to existing customers as soon as the codes became available. Also, the owners of all new bank accounts opened from January 01, 2011, should be provided with NUBAN code at the onset. The NUBAN scheme requires that the account number field in the cheque MICR code line should feature only NUBAN numbers. Accordingly, all new cheque issued to customers should carry NUBAN codes. With this transition method, the present account numbers and NUBAN codes would co-exist in the electronic payment and cheque clearing systems from January 2011 to June 2011. This implies that banks have to build in the required intelligence in their respective in-clearing systems to distinguish NUBAN codes from old account numbers while processing inward cheque items and electronic payment instruments, during this period.

The CBN said that before arriving at the decision, it consulted with three major providers of Core Banking Applications in the banking system to ascertain the feasibility of a uniform account number standard and the feasible implementation modalities.

It said that based on the technical advice obtained, it mandated a period of nine months for full compliance by the banks, adding that compliance monitoring by the Payments System Policy and Oversight Office would commence six months from the release date of the document.

CBN said: All banks are expected to submit their comprehensive migration plans to the Central Bank of Nigeria one month from the release date herein. Any infractions to the dictates and stringent time-lines provided in this document shall attract severe sanctions as may be determined by the Central Bank of Nigeria from time to time.

The Bankers Clearing House has witnessed an upsurge in the volume of automated direct credits cleared through the system since February, 2009. This resulted from the directive of the Federal Government to the effect that all Ministries, Departments and Agencies of the Federal Government should replace all forms of cheque payments with electronic payments as from January 01, 2009.

As the ACH volume increased, so have complaints of banks and bank customers resulting from the incidents of abuse of the clearing system. Such of the complaints include: delayed presentment of customers instructions in the clearing house; delayed application of inward automated direct credits items by some banks; late return of un-applied inward ACH items; application of inward ACH items to wrong accounts; bank customers quote account numbers wrongly.

CAWG observed that many of these complaints are traceable to the non-uniform structure of bank account numbers among Nigerian banks. For instance most ACH beneficiaries quote their bank account numbers wrongly while providing such account numbers to their employers, in preparation for electronic means of salary payment.

When this happens, both the employer and the presenting bank would not be able to validate such accounts before presenting such payment instructions through the Automated Clearing House.

A uniform account number structure scheme would enable both the employer and the presenting bank to validate account numbers and this would greatly reduce: the volume of items returned un-applied due to wrong account numbers; the incidence of posting to wrong account numbers, by the receiving bank; the incidence of delayed presentment of outward ACH items.

Presently, most banks use days to cross-check, validate and correct account numbers before presenting ACH items through the Automated Clearing House; the incidence of delayed application of inward ACH items.

Most banks expend a lot of energy and time to correct account numbers before uploading inward items just because their core banking applications work with too long bank account numbers. We are of the opinion that if the Nigerian banking industry implements a Uniform Bank Account Number scheme, then many of the electronic payment problems we currently experience would be resolved and banks would experience reduced cost of operations and increased efficiency of ACH processing.

The CBN directive added: In the course of our study and deliberations, CAWG discovered that Uniform Bank Account Number scheme is best practice. The proposed NUBAN is a 10-digit Bank Account Number format, with the following structure: 999999999 – Account Serial Number 9 – A Check Digit constructed to support a modulus check, which enables the presenting bank to perform checks.

The Check Digit is derived from an algorithm that operates on a combination of the three-digit CBN-assigned Bank Code and the nine-digit Account Serial Number.

Customer records database

Every bank is required to create and maintain a NUBAN code for every customer account (current, savings, etc) in its customer records database, and the NUBAN code should be the only Account Number to be used at all interfaces with a bank customer.

We expect every bank to maintain their present Account Numbers and use them for their internal operations only as from the effective date of NUBAN, but every such account number would have to be mapped to a NUBAN code as an Alternate Account Number.

The bank customer should be provided with only the NUBAN code which he/she would use as a means of account identity at every interaction with the bank. The onus lies on the bank to map such NUBAN code supplied by the customer to the relevant internal account number within the bank technology system.

A 10-digit account number is simple and can easily be managed by bank customers. NUBAN frees bank customers from the risk of quoting account numbers wrongly, a risk that is higher with account numbers of longer digits.

The NUBAN shall be used in ACH operations. Every payer shall obtain the three-digit Bank Code and a 10-digit NUBAN code from the payee whenever ACH payments are to be set up; the Payer bank shall ensure that all payee accounts supplied by the payer conform to NUBAN standards.

The Payer shall validate the check digit of the NUBAN code of every electronic payment instruction, and only instructions with valid NUBAN codes shall be presented in the Automated Clearing House; the receiving (Payee) Bank shall upload inward ACH payments based only on the NUBAN codes of each payment instruction; such upload programme/software shall validate the check digit (10th digit) of the NUBAN code in the upload process.

All inward items with invalid NUBAN codes shall be returned unapplied, and the receiving bank shall not make any manual effort to correct such records. d) The Account Number field in the MICR code line of cheques shall contain only the NUBAN code.

2.5 **DIFFERENCES BETWEEN BVN AND NUBAN**

A lot of question has been raised about the essence of Bank Verification Number (BVN) when there is already a Nigerian Uniform Bank Account Number (NUBAN). Does this imply that NUBAN is no longer effective? Before an answer is given to the above question, it is important to understand the two

concepts.

BVN is a biometrics identification of customers in the financial industry launched by the Central Bank of Nigeria (CBN) in February 2014, which is aimed at revolutionising the payment system in the country. The introduction of BVN authentication is targeted at addressing cyber crime, ATM fraud and other kinds of financial frauds as well as to safeguard customers’ funds to avoid losses through compromise of Personal Identification Numbers (PIN).

According to Isaac Okoroafor, acting director, corporate communications, CBN, BVN is a number that enables one person to have a single identity within the financial system. “We came up with this to achieve a few things; people who cannot read and write to use their biometrics which cannot be replicated, to tackle incidence of identity theft and enable banks to really identify their customers in the overall context of Know Your Customer (KYC) initiative,” Okoroafor says.

The NUBAN is a 10-digit bank account numbering system that is simpler to use than traditional longer account numbering structures, and is in line with requirements of the West Africa Monetary Institute, towards the economic integration of ECOWAS countries.

Every bank is required to create and maintain a NUBAN code for every customer account (current, savings, etc.) in its customer records database, and the NUBAN code would be the only account number to be used at all interfaces with a bank customer.

The CBN released the guidelines on NUBAN scheme in August 2010, to achieve uniform customer bank account numbering structure among all Deposit Money Banks in Nigeria, within nine months of that period. NUBAN has great potentials to resolve the observed problems with electronic payments in Nigeria, as many of them are related to specification of wrong beneficiary account numbers.

However, a number of operational modalities were released to the market by the CBN, to facilitate smooth and successful implementation of the scheme. As of today, the NUBAN project has been completely carried out by banks as every account holder has a NUBAN number.

Responding to the above question, OluseyiAdenmosun, biometric project, Nigeria Inter-Bank Settlement System (NIBSS) plc, explaines that BVN identifies you across the banking industry, while NUBAN identifies you in your bank, saying “NUBAN is NUBAN, and BVN is BVN. Banks verification number identifies you across the industry. NUBAN identifies you in your bank. We

are not changing anything. NUBAN stays, BVN stays, they do separate things even though they look similar.”

To him, every bank has a server that warehouses all the database of all their account holders that have a BVN and even the banking network has branches, each bank branch will connect to that server, do the enrolment and that server pushes the data to the NIBSS.

“At NIBSS, we search through our own system, find out if there is a march, if there is no march, we will issue a BVN which we will go back to pick up. If there is a march, we will alert the bank to be aware that there is something suspicious and so the banks can take much more informed decisions,” says Adenmosun.

Explaining the reason for BVN, Okoroafor says: “The incidence of fraud in the banking system, identity theft, even the challenges that has to do with the inadequacies in our country and trying to situate this in the context of financial inclusion, and we realise that because so many people are not educated – they cannot read and write, they are unable to key effectively into the cashless policy and electronic banking policy.

“So, the bankers committee came up with a one bullet solution that will take care of these – that will check fraud, prevent identity theft, and make ordinary people who cannot read and write to also make financial transactions, and we came to realisation that we can do a few things to help solve some of these financial challenges in our financial system, the bank came up with this BVN.”

**CONCEPTUAL ISSUES**

**THE HISTORICAL DEVELOPMENT OF COMPUTER IN BANKING INDUSTRY**

The ability of an organization to prosper and survive requires that its competitive position should not be significantly less than those of other firms operating within the same market sector. Hence computer technology has come to be accepted as an indispensable innovation in the banking industry as in most other fields of human endeavour like science, manufacturing, process control, research, education, artificial intelligence, etc. The reason for the ever-widening scope of acceptance and utilization is because the digital equipment is an all-purpose machine that can be selectively programmed to carryout a wide range of task. Accordingly the growth of the computer industry has been monumental, phenomenal and it has become the fastest growing industry to date.

The use of computer is still very new in our society. The emergence of computer technology dates back to late 1940s in the advanced countries of America and Europe and introduced into Nigeria in the 1970’s by the multinational corporations like UAC, NCR etc. while the banks embraced it in the early 80’s (Aweniemobor, 1991).

In the 1980’s, the processing of information in Nigeria was based on the centralized, architecture with a mainframe computer running a multi-user operating system and various users connected to it via terminals. This type of processing later changed to a more decentralized approach with local Area Networks (LAN) within bank branches. Recently, the application of modern technology has affected all aspects of the nation’s banking industry from the standard retail operating, such as cash withdrawal and cheque processing to the creation and delivery of sophisticated product, such as foreign exchange swaps.

The electronic revolution in Nigeria banking sector started sometimes in the early 1990s. However, the first visible form of electronic innovation in the nation’s banking industry was the introduction of ATMs in the early 1980 by a commercial bank in the country. Some other banks followed the bank’s experiences but the product was not well received by the banking community and this no doubt curtailed its spread in the early 80s (S.A. Ohiyemi).

However, it is interesting to note that PC-banking or desktop banking, was mainly popular among bank’s corporate customers rather than their retail customers. The electronic money product was later introduced. This was mainly in form of stored value cards operated by bank via valuecard and Gemcard companies. Both have been in market place for some time now (A.B. Zarma, 2001:72). The above overwhelming development made automation no longer a play thing or luxury but an indispensable part of every right, reasonable and forward thinking bank management.

The beauty of the advance technological growth in the banking industry is also deterred with the paralleled growth in its abuses. In Britain the “plastic fraud” in 1990 costs the British bank (100m) one hundred million pound (Business Time October, 19, 1992). In the USA alone in 1985 estimate put ATM fraud losses at ($200 million) two hundred Million dollars (the bankers’ magazine October, 1985).

First Bank business and economic report holds that computer fraud is not only rising in value but is becoming more sophisticated. As computers grow in number – incidence of computer fraud has started to move away from a technological variety of computer book-keeping fraud to more sophisticated scam. But as criminals become more adopt at penetrating computer networks, and as more and more non-bank participants join in money transmission networks. There is a real danger that fraud could rock both the local and international that fraud could roc both the local and international monetary system in this 21st century of the trend goes like this unchecked.

**NATURE OF FRAUD**

It is very common among people to take errors for fraud. Errors are not frauds. An error is simply a mistake that is inadvertent. It may take the form of an unintentional misstatement or an omission.

While fraud is an intentional act in a form irregularity or impropriety involving the use of deception to obtain an unjust or illegal financial advantage. Fraud could be as a result of the following:

* + - 1. Carelessness or negligence in a statement.
      2. False statement that have honestly been believed by the person making them.
      3. The deceit of a person not resulting in anyone else being misled (Okolie, 2004:67).

**WHAT IS FRAUD?**

Fraud is wide in its connotation and because of its diverse nature; it has been difficult to proffer a comprehensive and all embracing definition of the term **“FRAUD”.**

The Lexicon Webster’s Dictionary of English Language (1988.45) defines fraud as the use of deception for unlawful gains and unjust advantage; something that constitutes a crime, deception, someone who is not what he pretends to be.

The Oxford Advanced Learner’s Dictionary of Current English (1991:343) defined fraud as a criminal deception; someone who deceives people. The (1993:490) defined fraud also as an act of deceiving somebody illegally in order to make money or rather to obtain goods.

According to the Chartered Institute of Public Finance and Accounting (UK), defined fraud as those intentional distortion of financial statement or other records which are carried out to conceal the misappropriation of assets or otherwise for gain (Andre, 1997:50).

The international Auditing Guidelines (IAG) defined fraud as a particular type of originality involving the use of deceits to obtain an illegal or unjust advantage and may involve the following:

1. Manipulation, falsification or alteration of records or documents.
2. Misappropriation of assets.
3. Recording transactions without facts.
4. Suppressing or omitting transaction from records and
5. Misapplication of accounting policies.

Some Nigerian authors have also flexed their academic muscles in this area. Professor Nwankwo (1991), defined fraud as a complex universal phenomenon. He said it is rampant in both the developed and developing countries and varies across time and place in its magnitude, its sources the way it manifest, it effect are cumulative and circular and they extend beyond the boundaries of the nation and states.

Okafor (2003) opined that fraud involves deception for personal financial gains, which centres on some forms of trading and business organization between groups of people. Following this definition, and the propensity of the average human beings, to chest, it is substantial and favourably an argument, to say that fraud dates back to the beginning of commercial trading. One can easily say or infer from this that “fraud is as old as trade” and is considerably older than money itself and with the advent of money, we will then say that a whole new area for fraud was opened.

Successful frauds will not only result in a direct financial loss for the institution and banking sector, but, when reported in the media, will detract form confidence in the institution and the banking system in general.

Today, it is reality that fraud is notoriously difficult to investigate and prosecute. For one thing, frauds result in a huge financial loss to banks and their customers, the depletion of shareholders, “funds and bank” capital base, as well as loss of confidence in banks. For another, the incidence of fraud and forgeries could in the limit, lead to the closure of some affected banks as had happened in some parts of the world. The subject is therefore of special concern to the monetary and supervisory authorities who are concerned about the safety of individual banks and the soundness of the banking system. In the corporate context, fraud can be categorized as internal – committed by insiders (e.g. officers directors, employees and agents); and external when committed by outsiders such as (vendors, contractors, and suppliers). Corporate fraud can also be classified as crimes committed by insider against the company (e.g. theft, corruption and embezzlement); and crime committed by insider for the company (e.g. violation of government laws). Fraud is indeed broad and complex.

In a causative context, fraud is both personal and environmental. For example, economic need or greed generally motivates fraud perpetrators.

Environmental need that breed internal fraud and create opportunities and embezzlement and theft include Lax accounting controls. Fraud as a phenomenon is not new, neither is it peculiar to some industries, what is new about fraud is the increasing uncontrollable wave since the mid 1980, when most Nigerians desired to get rich quickly without working, a development that undermined the concept of “dignity in labour”. Any organization that desires long-term survival and growth must articulate and manage its resources adequately to avoid corporate failure.

What is central here is that the definition of fraud varies widely in nature but it can be summarized as the misappropriation and misrepresentation of firms or persons, facts and figures for personal gains.

**TYPES OF FRAUD**

We shall first of all take a general look into the types of fraud, before we go into those that are peculiar to banks. A.O. Okolie in his book; “Practical Guide to Financial Investigations” puts forward 6 (six) types of fraud. They are:

1. **STEALING (OR LARCENY)**

Stealing is when a person, fraudulently and without claim of right in good faith, takes and carried away anything capable of being stolen with intent, without the consent of the owners, at the time of such taking permanently to deprive the owners thereof. A lawful possession of items as a bailer or part owner will not amount to stealing, but if a person fraudulently convert the items to his own, or the use of any person other than the owner’s part he will be guilty of LARCENY.

2. **EMBEZZLEMENT**

A person may be guilty of embezzlement if he is an employee or under the service of a person or organization and:

a. Steals any chatted, money or valuable security belonging to or in the possession or in the power of his employer or master or,

b. Fraudulently takes away (without due consent) part of, or the whole of any chatted, or money or valuable security delivered to him or received or taken into possession by him or in the name or an account of his master or employer.

The following conditions must be present for a fraud to be called embezzlement:

* 1. The defendant must be an employee of an organization or servant in the service of this master not merely on aged.
  2. The item or property must be received for or on behalf of his master or employer and then intercepted.
  3. There must be a fraudulent appropriation of property or item in question. This means that carelessness resulting in making incomplete accounting entry or a delay in paying over money may not amount to embezzlement.

1. **FALSIFICATION OF ACCOUNTS**

Falsification of account is usually committed by persons acting in the capacity of a clerk, an officer or a servant employed by a person or an organization. It usually takes the nature of willful or deliberate (with the intention of defrauding) destruction, alteration of any book of account, paper, writing or valuable security or account which belongs to or it in the possession of the employer or has been received by him for or on behalf of his employer.

A person may be guilty also, if falsification charge if he makes or consent in committing or making any false entry in or any deliberate omission or alteration of any materials, books, records, documents, or account.

This charge is a scoop-up covering such fraud as bad debts falsification, falsification of write-of-that are unwarranted, over-valuation of stocks etc. Fraudulent adjustment of a computer will result to fraud of falsification since this can be through mechanic or electronic means of rendering accounts.

1. **FORGERY**

This is the preparation of false document with a view of using it as genuine. This can also be seen as the fraudulent imitation of a signature, document, etc. There is usually intent to deceive or defraud with such a document. As at 1999 – 2003, using the NDIC report, the highest reported incidence of frauds and forgeries occurred in ten banks and the banks were responsible for a large percentage of the total amount involved. The following are the commonest types of fraud and forgeries:

* 1. Presentation of forged cheques and dividend warrants.
  2. Granting of unauthorized loans
  3. Posting of fictitious credits
  4. Suppression of cheques; and defalcations
  5. Fraudulent transfer and withdrawals.
  6. Loss of money to armed robbers and outright theft of money.

1. **FRAUDULENT CONVERSION**

A person may be guilty of an offence of being in possession of a property intended for someone and fraudulently depriving that person from using/enjoying from it. More often than not, fraudulent conversion applies particularly to company directors, or members and officers of a corporate body using the organizations properties. What one would have called embezzlement, if the defendants were a servant or clerk of a company may be a fraudulent conversion, if the defendant is a member, director or officer of the organization.

6. **FALSE PRETENCE**

In the case of false pretence, an existing fact, and not necessarily by words, is a condition precedent to establishing a fraud. For example, if a person puts on an Army Uniform, or better still, NYSC uniform, when he or she is not a military man or a corper and obtains benefit in values, as a result, he may be guilty of a charge of false pretence. This may be correctly called IMPERSONATION and it is a criminal offense and punishable by law.

**NATURE OF COMPUTER FRAUD**

Input operations, data processing, output operations, and communications have all been utilized for illicit purposes. The more common types of computer related crimes are categorized here. Fraud by computer manipulation intangible assets that are represented in data format, such as money-on-deposit are most common targets of computer relation frauds in banks. Examples of computer fraud are as follows:

1. Data diddling
2. Trojan horse
3. Salami technique
4. Computer forgery
5. Desk top counterfeiting
6. Teeming and lading or carry over fraud.

**DATA DIDDLING:** According to Joseph T. Wells (2003), this is an input manipulation of computer fraud. It is easily perpetrated and difficult to detect. It involves the deliberate entity of false information. It does not require any sophisticated computer knowledge and can be committed by anyone having access to normal data processing function at the input state.

**TROJAN HORSE:** Joseph T. Wells (2003) states that Trojan horse is an example of a common method of programme manipulation used by persons with specialized knowledge of computer programming. It is a processing stage fraud, which is very difficult to discover and is frequently not recognized; it involves changing existing programmes in the computer system or inserting new programs or routines.

**SALAMI TECHNIQUE:** This is a particular specie of fraud conducted by computer manipulation that takes advantage of the automatic repetition of computer transactions. It involves the nearly unnoticeable “thin slices” of financial transactions, they are repeatedly removed and transferred to another account. According to Adamu Osumah et al (1997:19), account which have been dormant for quite some time (i.e. account which have not been serviced) are normally used as the account through which such slice amount are gathered and subsequently withdrawn by the fraudster.

**COMPUTER FORGERY:** This is a type of computer fraud, which occurs when a perpetrator alters documents stored in a computerized form. In this instance computer systems are the target of criminal activity.

**DESK TOP COUNTERFEITING:** A new generation of fraudulent alteration or counterfeiting emerged when computerized colour laser copiers became available. This was opined by Joseph T. Wells, chairman and founder of the Association of Certified Fraud Examiners (ACFE) Texas. These copiers are capable of high resolution copying; modification of documents, and even creation of false documents without benefit of an original. They produce documents whose quality is indistinguishable from that of authentic document except by an expert. These schemes takes very little computer knowledge to perpetrate. Counterfeit cheque, invoices and stationary can be produced using scanners, colour printers and graphic software.

**TEEMING AND LADING OR CARRY OVER FRAUD:** This is a situation whereby a cashier may authorize borrowing of client balances. It usually occurs in the case of newly opened large balance account to be corrected through the system override facility.

When customers complain, it will be blamed on data processing error often with the promise of rectification, money is then moved from one account to another to hide the discrepancy or the actual cash siphoned.

The significance of this is that most employees see it as the safest means of meeting their financial commitment often with the intention of paying back.

**TYPES OF FRAUD PERCULIAR TO BANKS**

The fear is now rife that the increasing wave of fraud and forgeries in our banks in recent years, if not arrested, might pose certain threats to the stability and survival of individual banks and the performance of the industry as a whole. This has led to people feeling that fraud is only associated with banks. For one thing, Frauds result in huge financial losses to banks and their customers, the depletion of shareholders fund and banks capital base as well as loss of confidence in banks. And sometimes it leads to the closure of affected banks. Fraud is a complex universal phenomenon. However, there is no where fraud is more common than the banking industry. It has also been proved to be the biggest single course of bank failure. In the past, banking was almost a religion with bank employees so dedicated that the watchword in the banking industry was transparent honesty. With the current wave of bank fraud and forgeries, one may not be too wrong to say that it seems that those good old days are gone. Then what are the types of frauds peculiar to banks?

Nwankwo (1991) in his book; “Bank management, principle and practice”, classified fraud in three ways namely:

1. By flow
2. By victim, and
3. By the nets

**THE FLOW FRAUDS:** There are two types of flow frauds, smash and grab and the other drip. Smash land grab are usually small in numbers, high involve and occurs over a very short period of time. They usually take the form of electronic funds transfers, security fund transfers, or theft through vault break-in or in the mid-air. Drip type of fraud occurs through by passing of routine controls and employing large number of fraudulent act each of relatively low value. Each fraud is repetitive in nature and may be operated successfully for a number of years without detection. Techniques used in drip fraud include payroll padding through which ghost workers receive payments and Salami operations where fraudulent programmes are used to credit small rounding differences to a favoured account.

**FRAUD TYPIFIED BY THE VICTIM:** Victim fraud are those classified or identified by the victim of the fraud for instance, in terms of those committed against the company or bank itself and those committed against parties outside the bank. Fraud against parties outside the bank include fraud committed by employee, directors, or the board-indeed the company itself against shareholder, other vestures, financial and trade creditors, depositors the regulatory authorities, etc.

**ACT FRAUDS**:Bank frauds can also be classified in another way one is by the perpetrators, by the instruments or by the method used:

**PERPETRATORS FRAUDS**:As the name implies are those classified as such by the group or individuals committing the frauds which includes employee’s and corporate frauds and also by outsiders

**FRAUDS BY METHOD**: This very kind of fraud takes many forms:

i. **EFTOS FRAUDS:** One is electronic funds transfer (EFTOS) fraud. This kind of fraud has been facilitated by the increase in the volume and value of the payment traffic passing through the inter bank transmission payment systems by new technology’s particularly the computer, and by the increase and modernization of the banking computer networks and the widespread use of ATMS, all of which have made the financial system more unworkable to a wide variety of vandalism and fraud computerization, by its very nature. It makes fraud easier to commit, harder to detect and exploitable by more people. For successful fraudsters, the rewards can be enormous and risk small (Financial Times, London 28 November, 1985).

Only a few years ago, access to confidential and financial data held on computers was restricted to a chosen few senior executives and technical personnel. But today, with the massive expansion of computerization, brought about by the desk to machines, large numbers of junior staff are joining these selected groups. The computer has spread the availability of proprietary information to a degree that until recently would have been considered unthinkable. Accordingly employees who would never before have dreamt of stealing corporate property are tempted by new and confusing resources and opportunities. Being in possession and control of data that competitors and speculators are eager to acquire, and of resources funds – that everybody requires can work miracles. To further support this Prof. Nwankwo quoted Roy Carter, “who emphasized, “overnight, this transforms ordinary people into influential ones and poor people into affluent ones. The temptations are often enormous, compared to the intangible even innocent nature of the crime involved and the low level of risk”. In most computer system, large numbers of people have access to the same data at various random points along the line of communication. This actually leads the criminal to believe, often rightly, that any manipulation or theft of data will not be traceable to him, even if detected. In other words, he feels no danger of leaving his finger prints at the scene of the crime.

Finally, the fear of unfavourable publicity adverse shareholder reaction or the disclosure of confidential matters often means that proven cases are not reported as an ordinary theft might be.

EFTO frauds usually result from totally false messages created for the sole purpose of fraud or through alteration to genuine messages such as changing the beneficiary’s name, account number or increases in the amount transferred. They can also occur through theft e.g. of a credit card or ATM card and pin number belonging to someone else using it for transfer cash funds. Or through the form of a bad ATM machine, withdrawing a huge sum of money which does not reflect in his Account.

Many of the EFTOS fraud transcend international boundaries and are initiated on a day before a public holiday in the sending bank country (which might be a working day for the receiving bank). This then gives the perpetrators extra time to convert the funds and escape. Many EFTO frauds are unreported because no bank will talk to you about fraud. They don’t want to scare away investors or encourage other people to try the same thing. Some ideas of the magnitude can however, be gained from some of the few reported in the press. One of such report is the case of three students who are presently in the net of the EFCC. They allegedly withdrew about N34 million Naira fraudulently from a Bank account through a faulty ATM machine (July 2008).

**TYPES OF LOAN FRAUDS**

|  |  |
| --- | --- |
| Borrower | Provides false information to the loan officer pays bribe to the loan officer unconcealed financial interest by the loan officer. |
| Loan officer | Falsifies records and rolls over advances to conceal bad debt. |
| Bank | Lends to ghost companies falsifies book-keeping records. |
| Borrower | Offers fraudulent collateral, security, documents. |

ii. **Fraudulent Loans:** Banks are frequently victims of defaulting and fraudulent loans. Loans may be made to be fictitious or ghost entries, to genuine borrowers or to entities which the lending officers has an interest it can be made directly by the lending bank or through a participation syndicate involving other financial institutions. The loan may be secured.

**COMPUTER FRAUD IN BANKS**

Banks have always been exposed to risk such as error and fraud but the scale of these risks and the speed with which they can arise has been accentuated in geometric proportion to the speed of technological innovation in computers telecommunication systems. More and more, the integration of automated operations are increasing the dependence of banks on the reliability and of their Electric Data Processing (ED) system.

Today, the need to protect computer systems has been strongly advocated, in views to their strategic importance. The reasons are five-fold.

The first is the ease with which information can be lost in a computer. This may be caused by unintentional error by the operator.

Secondly, malicious damage to data is becoming rampant and easy to perpetrate. So also is the problem of unauthorized access to the system.

Thirdly, the intended and unintended consequences, of security breaches can be enormous. This is costly in time and money and may result in loss of goodwill to the organizations.

Fourthly, computer and telecommunication ensure large amount of personal and confidential information to be available on line to diverse users with various intentions. This has posed some ethical and social problems concerning privacy of individual information.

Fifthly, computers complicate the problem of accountability of staff responsible for handling sensitive information. This is more so under a computerized system since information can be compromised from remote places without the active connivance of staff.

It is in view of these considerations that issues pertaining to various aspects of a computer based system must be addressed – hardware software, communication, operation and personnel.

**FRAUD AS A COMPUTER ABUSE**

A.E. Awenlinmobor (1991:24) opines that data flows in banking represent assets or instructions which ultimately move asset. Successful frauds, will not only result in a direct financial loss for the institution but when reported in the media will detract from confidence in the institution and in the banking system in general.

However, going through the corridor of history you will find out that some smart herds have been fraudulently manipulating the use of computer in banks all over the world.

Adamu Osuma et al (1997:23) disclosed in their work the biggest bank fraud which come in Los Angeles on November 3, 1978. Some one taped the bank system, transferring funds to other bank to the tune of 10 million dollars. This as the FBI (Federal Bureau of Information) put it Rifkin parlayed his sophisticated knowledge of electronic and computer into one of the biggest ban theft in the history.

The fraud happened tin security pacific bank, the 10th largest bank in the United State of America. Rifkin on the pretext of checking out the bank computers, gained access to all the important transferring. He was known to bank personnel and so, no one questioned his right to be in the computer room. But they did not know that he apparently had the identification number of a bank official. This coupled with his knowledge of the daily code number and using the fake name of “Mike Hamson” made it possible for him to order $10.2 million dollars been transferred to Hamsen’s account in the living trust corporation of New York. From there money was transferred to the Swiss account of the Russian Diamond Five, Russ ELMAX in Zurich.

Adamu Osumah et al (1997:24) also observed that for the transfer to be possible, it requires three secret codes, which the fraudster was equipped with. One for the account being looted another for the personal identification of an authorized bank official and finally the special security code, which is changed once a day, at times on hourly basis.

It is important to know that the transfer was made at the close of the working day. Thus the fraudster caught the staff at a low level of security alertness. In other words, they were clock-watching instead of money watching.

A confessional statement from Adamu Osumah et al (1997:24) “I took $1.5 million dollars from Union Dine Savings Bank in new York and the bank never seemed to miss a penny file”. Only for the original to be destroyed accidentally microchip can be used fraudulently to copy file if access to computer storage room is not restricted.

Inspite of the computerized accounting system in Nigeria banks since 90’s there seems to be an increase in reported cases of fraud in Nigeria banking institution. According to the NDIC Annual report and financial statement 2001, the average number of reporting banks during the year stored at 75 as against 63 in the previous years. Reported cases of fraud increase significantly from 403 cases to 943 in 2001 depicting about 134% increase as a result there was a significant increase in the total amount involved. From about N2.851 billion in 2000 to N11.244 billion in 2001 representing an increase of almost 300%. On the other hand, the expected loss was estimated at N906.3 million as at December, 2001 compared to N2,080.57 million in 2000.

Beside the above succeeded cases of fraud, there are also attempted cases of fraud that were uncovered.

According to Professor Okoh S.E. et al (2003:21), one Emmanuel Ofuasia a staff of First Bank of Nigeria Plc bought a bank draft No. 000986 for N50, drawn at Abibu Oki Branch Lagos in faovur of his wife.

The story has it that the purpose of the purchase of the N50 draft was to enable the fraudsters master the signatures on the bank draft and to print and photocopy a replica of the draft. However, luck ran out against them when the police (a “Crack anti-fraud team) from Asaba swiftly moved to New Nigeria Bank plc in Okpanam in the early hours of January 21st 1990 to forestall the deal. Again it is not unknown for computer hackers to steal from banks and finance houses by electronically transferring funds until they reach an of shore account. In U.S.A. alone in 1985, estimate puts A.T.M. fraud losses at N200 million dollars first bank monthly business and economic report (April 1995:11). Just recently (2008) three students of Ambrose Ali University Ekpoma were arrested by the Nigeria police special fraud unit (STU) Milverton Road, Ikoyi, who are presently in the custody of the EFCC.

They withdrew the sum of N34 million fraudulently from a Bank account through a faulty ATM machine. The fraud was detected at the Benin Branch of Access Bank Nigeria Plc.

**STAGES OF COMPUTER FRAUD IN BANKS**

In this section, focus is on identifying the stages the aforementioned fraud can take place. Since the uses of computer involves three stages, input, processing and the output stage.

**THE INPUT STAGE**

This is the stage at which data to be processed are made available or read into the system.

Looking also at banks which uses computer system a situation where information from a transaction is keyed directly into the computer through the (VDU) is good enough to check. The obvious deduction here is that it is possible to alter figures. It is also possible to mistakenly key in the wrong figures.

**PROCESSING / PROGRAMME STATE**

Richard Oghuma et al (2002), states that every operation performed by the computer is in accordance with the pre-defined instruction installed in the computer called programme. The processing of information by the computer is based on the programme logic and the inputed data. Hence, computer could be described as a robot which works according to institution, garbage in garbage out (GIGA). Thus a situation where the output is different from input, insinuate that fraud have been conceived by an employee.

Furthermore, situation where there is no separation of duty of programmes who design and construct the programme input preparation and the operation at the computer, fraud will be inevitable. It can also be possible for unauthorized programme to go through the computer. “Trojan horsing” the possibility also exist for input and output files which are not properly stored or secured to be stolen or damaged. These loophole in any case are serious avenues for fraud.

Hence, so many internal measures have been employed to arrest the situation. Finally, the computer as we know operates in a given environment condition (electricity, clean environment air conditioning) or which the absence will course a lot of damage to data. The loss of electricity for example can ruin a wide computer department. Also the unavailability or inadequacies in cooling the equipment, the question then becomes, is it possible for fraud to crop up and covered up with lack of power supply from NEPA now known as PHCN or faulty air condition? The obvious answer is that it is possible.

However, the inadequacies can be provided for with the use of mini uninterrupted power supply (UPS) and central cooling system. In this stage, therefore, the destruction of files and falsification of data and programme should be expected.

**OUTPUT STAGE**

Frauds occur at this stage by targeting the output of the computer system for example cash dispenser fraud”. This fraud is achieved by falsifying instruction to the computer in the input stage. Usually with the use of stolen bank cards.

Richard Oghuma (2002), hese stage allows the result of data processing to be transferred, communicated or related to the outside world. E.g. example of output devices are visual display unit (VDU) or monitor, printer and plotter, output can be created for two purposes.

1. Providing usable information for communication.
2. Providing output to be filed for a later use.

However, a critical look at these measures will reveal that it is not as easy as it sounds. Because by the nature of most computer, they are providing a continuously online service to their end users throughout the working day. The computer and its files are thus exposed to any mishap that may occur, but its operate error, equipment breakdown, power failure, programme error and even deliberate manipulations.

Situation whereby data has been deliberately manipulated before passing through the computer there is no doubt that the output will be carrying some misleading result since the data used are contaminated. The computer has no defense against situation like this which stem from the fact that only few computers has the in-built facility which automatically detect errors of this nature. In another case the disc master file can equally be copied with amendment as duplicate or backup.

**CONTROL OF COMPUTER FRAUDS**

Information available to us shows that fraud has been and is still a major problem in the Nigeria banking sector and management has been in the forefront of controlling fraud in a computerized system. Professor Okoh S.E.N. et al (2003:122) states that the statistics of frauds and forgeries in our lands today perpetrated primarily by bank workers.

Prof. G.O. Nwankwo (1991:181) disclosed that insiders usually in collusion with outside third parties commit most frauds. The NDIC Annual report and financial statement (2001:33) revealed the total of 152 staff of banks involved in fraud and forgeries in 2001, core operations staff such as supervisors, officers, accountants, managers, executive assistants, clerks, and cashiers accounted for about 95.4 percent and increase of 20.3 percentage points relative to the previous year’s level.

**POLICIES CONTROL**

From the above discussion of the anatomy of frauds management should evolve positive policies towards safe-guarding the banks assets and ensuring that staff do not exploit weakness in internal control policies as follows:

1. The policy should stress the cardinal principles of separation of duties to ensure that one person does not originate and complete an assignment or entry.
2. It should also emphasize dual control of sensitive areas such as strong rooms and locks to security documents.
3. Other preventive measures to be enshrined and emphasized in the policy include the separation of life and dormant accounts.
4. The treatment of overdrawn and dormant accounts.
5. The need for daily balancing and periodic reconciliation of accounts including clearing and correspondent account.
6. There should be precautions and procedures including necessary references, for opening accounts.
7. There should be need for full compliance with established policies rules and procedures with exceptional desirable duly and appropriately authorized.
8. The banking industry should insist on honesty and dedication, that is to say employment should be based on integrity and merit and not be a dumping ground for morally debased unemployed fraudsters in the society.
9. The Central Bank of Nigeria 9CBN) and the National Deposit insurance corporation (NDIC) should hence forth publish the names of banks and the officers involved in frauds and forgeries in our national dailies.
10. Finally, the policy should incorporate and emphasize expeditious reporting investigation and possible prosecution of suspected frauds.

**TACTICAL CONTROL**

This forming control helps in preventing computer frauds, it is as follows: Design of system and the paraphernalia of protecting it, including a back-up system to allow for machine failure, cryptographic facilities to protect the computer data network and terminals from illicit access or tempering, or protecting services to prevent process, key management, recovery and contingency management, software and data integrity and security responsibilities. Each message must be authenticated end-to-end with the relevant keys, which must be appropriately secured. Power failures must be guarded against by providing uninterrupted power supplies through standby generator Prof. G.Ol. Nwankwo (1991:182).

**CHAPTER THREE**

**SYSTEM ANALYSIS AND DESIGN**

1. Introduction

This chapter takes an overviews on the system design and the entire research work, it is important to note that a poorly designed system will equally produce an incorrect output as such this chapter presents a skeletal approach to the design of the entire system.

3.1 Research Methodology

A software development methodology or system development methodology is a frame work that is used to structure, plan and control the process of developing an information system. The methodology employed for the development of the system is the spiral development. The spiral development model comprises the elements of both design and prototyping. The model has four stages namely:

* Planning
* Analysis
* Evaluation
* Development

The data used for the development of the research was gotten from the internet, textbooks and articles. The contributions of other researchers on the subject were examined so as to gather relevant information.

3.2 System Analysis

System analysis has to do with examining a system in order to understand its step by step operations so as to identify its benefits and areas of limitation that require improvements.

3.2.1 Analysis of the existing system

In the existing system, tourism is done manually. A typical example is that if a tourist comes in to Nigeria, he will need to ask people so many questions in order to know his way about.

3.2.2 Problems of the existing system

The problems of the existing system include; it is time consuming, customers go through a lot of stress just to fill and submit the enrolment form.

3.2.3 Analysis of the proposed system

The proposed system is such that will help a bank customer to filland submit the BVN form online without going through the stress of queuing at the bank they are currently banking with. It also include submitting your biometric data after it has been captured by the newly developed system

3.2.3.1 Advantages of the proposed system

The advantages of the proposed system include; it will save time, it helps customers to submit their BVN biometric data at the comfort of their home. This will encourage customers to enroll in the ongoing BVN biometric data capturing exercise on their own without anybody persuading them to do so.

3.2.3.2 Disadvantages of the Proposed System

The major disadvantage of the proposed system is that an individual may be forced to submit his biometric data in place of others and some people may supply the wrong information if not guided on the right thing to do.

3.3 System Design

The system design pertains to the layout of the system and it consists of the input and output layout.

* + 1. Input Layout

3.3.2 Program Flowchart

See Appendix A

3.3.3 Output Format

See Appendix C

**CHAPTER FOUR**

**SYSTEM IMPLEMENTATION AND DOCUMENTATION**

1. Introduction

This chapter presents the system flow chart, analysis of modules, choice of programming language and programming environment.

4.1 System Design Diagram

Main Menu

Exit

BIOMETRICS DATA CAPTURING

REGISTRATION

SUBMIT

CANCEL

CANCEL

SUBMIT

4.2 Choice of Programming Language

The programming language chosen for the development of the system is PHP. The language was chosen because it enables fast implementation of complex solutions, it runs on practically any platform – not only on windows, but also, for example, on Linux, Unix, and IBM’s Systems, it also offers great flexibility during and after the initial project.

4.3 Programming Environment

This system can function effectively in windows such as: window XP, window 7 and window 8, etc. However, because of the structural concept of the language used, it is flexible for amendment in future when the need arises. More so, in order to accomplish or realize this research work, the following hardware and software components were used.

The hardware requirements are;

* Super video graphic array monitor
* At least 512 MB RAM
* At least 40 GB hard disk
* Keyboard
* Mouse
* Uninterruptible power supply (UPS)
* Fingerprint Machine
* Webcam
* Modem

The software requirements are:

* Server
* Browser

4.5 System Implementation

Implementation is the process of replacing the old system with the new system. There are four different ways of replacing the old system with the new system. The reasons for choosing one implementation type over another depend upon; how quickly must the changeover happen? How important is it to prevent data loss? What will the cost of the changeover be?

Direct changeover: In this system the old system is no longer available and everything must run on the new system. Problems with the new system can cause major problems for the business, only suitable for non-critical systems.

Phased implementation: Takes longer to complete the implementation but the risks to the business are less than for direct changeover. The new system can be split into separate working parts e.g. sales, marketing, payroll etc. part of the old system is replaced with the new one until the replaced part is working properly. Continue the process until the entire old system has been replaced by the new system.

Parallel Running: Highly fault tolerant, new system and the old system are used with extra staffs recruited to run the new system but it is very expensive. Both systems continue to run until the new system is working properly then the old one is discarded.

Pilot Running: If the business has many different offices or sites then this is an option. One single site is chosen and the old system is replaced with the new system in the same way as direct changeover but only on one site, the rest of the business continue to use the old system. Once the new system is shown to work well in that one ‘pilot’ site then the new system can replace the old one in the rest of the company.

The system implementation method recommended and chosen by the system developer is the parallel running so as to prevent data loss.

**CHAPTER FIVE**

**5.0 Introduction**

This chapter focuses on summary, conclusion and recommendations.

Here, the entire summary of the research from the problem stage to the implementation stage, the relevant conclusion and recommendations are discussed.

**5.1 Constraints of the Study**

The problems encountered during the course of carrying out this research project include:

1. **Time**: Time for the research project was too short coupled with researcher’s academic time table.

2. **Fund**:There was limited fund to take care of the research properly in terms of transportation and other expenses especially when visiting attraction sites.

3. **Research Materials:** Lack of access to research materials on the topic in the polytechnic library and even public libraries were also major constraint in the cause of this project.

**5.2 Summary**

Implementation of an online bank verification number system has been carried out with a biometric data capturing feature.

The existing method of queuing at the bank to collect and submit BVN enrolment form has been so stressful, time consuming and always at a high cost. The new system would be very easy to use because of its accuracy and reliability. Information about BVN andthe enrolment requirement can be promptly assessed easily.

**5.3 CONCLUSION**

BVN is a biometrics identification of customers in the financial industry launched by the Central Bank of Nigeria (CBN) in February 2014, which is aimed at revolutionizing the payment system in the country. An Online Bank Verification Number System for Nigerian banks was produced in this application. Through the new system, customers will be assigned a single identity within the financial system. It will help people who cannot read and read and write to use their biometrics which cannot be replicated, to tackle incidence of identity theft and enable banks to really identify their in the overall context of Know Your Cusomer (KYC) initiative.

**5.4 Recommendations**

Having designed, tested and implemented the new system, the following must be put in place to fully achieve the objective of which the software is designed.

1. **Maintenance:** The system needs to be maintained. This implies that any fault detected should be reported to the programmer for correction at any point in time.
2. **Internet Connection:** The system needs to be connected to the internet before the user can access the features of the software.
3. **Research:** More research should be conducted on the topic to assess it effectively.

**REFERENCES**

# Collins Nweze (2014) Bank Verification Number: For a safer, Better Banking

# Source: <http://www.financialtechnologyafrica.com/feature-articles/1716/bank-verification-number-for-a-safer-better-banking/>

# Eteyen M. Ekpeyong (2015):CBN’s Bank Verification Number

Hope Moses Ashike (2014) **:** Why bank verification number when there is NUBAN

Source: [http://businessdayonline.com/2014/04/why-bank-verification-number-when-there-is-nuban/#.VZTgxPlViko](http://businessdayonline.com/2014/04/why-bank-verification-number-when-there-is-nuban/" \l ".VZTgxPlViko)

curriculum", Journal of Retailing and Consumer Services*,* vol. 14, no. 4, pp. 289-295, 2007. Choi, J. Y., J. H. Jung, S. Park, H. J. Shin, and B. M. Chang, "A Smart Location-Aware Application

for Bus Guide based on GPS", International Journal of Information Processing and Management*,*

vol. 2, no. 1, pp. 101-108, 2011.

Huang, M. L. and J. H. Hong, "A Geospatial Service Approach towards the Development of a

Debris Flow Early-warning Systems", Advances in Information Sciences and Service Sciences*,*

vol. 2, no. 2, pp. 107-117, 2010.

De-hui Liu, “The application of GIS in tourism: discussion on tourism GIS and its research development and prospect,” Geomatics& Spatial Information Technology, vol. 31, no. 1, pp. 90-95, February 2008.

Hua-long Zhao, “GIS and its Application in Tourism Management,” Journal of Science of Teachers’ College and University, vol. 27, no. 3, pp.21, May 2007.

Ying- ying Li, De- liang Sun, and Jian- fang Yi, “Application and Development of GIS in Tourism Management,” Image Technology , no.4,pp.3-72006.

Juan Wang , Liang-song Zha , “Application of Multimedia and GIS Integration to Tourism Development,” Geospatial Information, vol. 3, no. 6, pp. 11-13, December 2005.

**JOURNALS**

Adam Osumah A. et al (1997). Computer Fraud in Bank.

Aigbokhaevbolo Oziegbe M. (2000). Fraud and Commercial Banks in Nigeria.

Annual Report and Account (1992). First Bank of Nigeria, Plc.

Annual Report and Account (2004). First Bank of Nigeria Plc.

Awake (2004). Protect Yourself from Fraud. July 22, pp. 4-10.

Awenhimobor, A.E. (1991). Computer in Banking usage and Abuses. NDIC Quarterly Vol. 1 No. 4.

Benedict E. Okafor (2003). Preventing Corporate Fraud. The Nigeria Accountant. October/December, 2003, Vol. 36. No.4.

Business Times Oct. 19. 1992.

Eddy Ndekwu C. (1994). First Bank of Nigeria. A Century of Banking. Spectrum Book Ltd. Ibadan.

First Bank Business and Economic Report, April 1995.

Erimafa J.T. Akpome, D.E.O. and Ikpotohin, F.O. (1997). Statistics for Undergraduates. Osasu Publishers. Benin City, 135 – 140.

Igudia, P.O. (2002) Statistics for Business and The Social Sciences. Imprint Services, Benin City. Pp. 136.

Joseph Wells, T. (2003). “The Computer as a Tool for Fraud Examiners” Austin Texas. A.C.F.E.

Murray R.S. (1992). Theory and Problem of Statistics. MC Graw-Hill International (UK) Ltd. 2nd Edition.

N.D.I.C. (2001) Annual Report and Financial Statement.

Nuamdi Asika (2002). Research Methodology in the Behaviour. Sciences. Lagos, Longman Nigeria Plc.

Oluyemi, S.A. (2001). Development of Electronic Banking in Nigeria. The Associated reputation/supervisory challenges. NDIC Quarterly Publication.

Okolie, R.O. (2004). Practical Guide to financial investigation. Sylva Publishing Akure.

Okoh, S.E.N. et al (2003). Banking in Nigeria: Mindex Publishing, Benin City.

Prof. Nwankwo G.O. (1991) Bank Management, Principle and Practice. Matthouse Press Ltd. Lagos, Nigeria.

Richard, Oghuma et al (2002). Fundamentals of Data Processing. New Era Publications. Benin City.

Yomere G.O. et al (1999) Research Methodology in Social Sciences and Education. Centrepiece Consultant Nigeria Ltd. Benin City, pp. 255.

Zarima A.B. (2001). Electronic Banking: Practices from other countries associated risk and implications. NDIC quarterly Vol. 1 No. 4.

**OBJECT CODE**

**HOME PAGE**

