AN ANALYSIS OF THE IMPACT OF INFORMATION TECHNOLOGY ON FRAUD IN NIGERIAN BANKS: A CASE STUDY OF BROAD BANK OF NIGERIA LIMTED

BY

ALIYU, Aishatu Doma
MBA/ADMIN/36222/2002-2003
(GO2/BAMP/7051)

BEING A PROJECT SUBMITTED TO THE POSTGRADUATE SCHOOL OF AHMADU BELLO UNIVERSITY, ZARIA IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION (MBA)

DEPARTMENT OF BUSINESS ADMINISTRATION
FACULTY OF ADMINISTRATION
AHMADU BELLO UNIVERSITY

November, 2005

DECLARATION

I hereby declare that this project entitled: An analysis of the impact of Information Technology on fraud in Nigerian banks – A case study of Broad Bank of Nigeria Limited (BBNL) is a product of my research findings. All relevant sources of information collected for the study are clearly acknowledged by means of references.

…… ……..

ALIYU AISHATU DOMA DATE

CERTIFICATION

This is to certify that this project titiled “An analysis of the impact of Information Technology on fraud in Nigerian banks : A case study of Broad Bank of Nigeria Limited (BBNL)” by ALIYU, Aishatu Doma meets the regulations governing the award of degree of Masters of Business Administration (MBA) of Ahmadu Bello University, Zaria and it is therefore approved for its contributions to knowledge, and literary presentation.

……	……..	……...
Mall. S. A. Karwai	Signature	Date
Chairperson, Supervisory Committee		
……	……..	……...
Dr. M. N. Maiturare	Signature	Date
Head of Department		
……	…….	…….
External Examiner	Signature	Date
……	…….	…….
Dean, Postgraduate School	Signature	Date

DEDICATION

I dedicate this project to my late grandmother, AMINYE – her selflessness and perpetual desire to unite people has greatly inspired me.

ACKNOWLEDGEMENT

All praise be o ALLAH the creator and sustainer of all things.

I wish to express my profound gratitude to my supervisor, Mallam S. A. Karwai for his guidance and dedication in ensuring that this project work is a success.

I wish to acknowledge the following people for their immense contribution in ensuring the successful completion of this endeavor: Mallam T. M. Yakubu, Mr. Deji Erinle, Mallam Inuwa (Shadow).

My appreciation goes to my dear friends, Fatima Musa(Mutimiya), Mr. Kwaghe (Chairman), Mr. Isaiah Bulus and the class of MBA 02/03 for all the support and encouragement as well as the friendship that has always being freely extended to me.

My gratitude also goes to all the lecturers and staff of the Department of Business Administration who have one way or the other contributed to ensuring that I am adequately groomed to take on the challenges of life.

Finally, I will like to thank all my family and friends for always being there for me. I feel honored to be associated with you all.

ABSTRACT

In recent times, financial institutions rely heavily on automated systems and electronic funds transfer network for majority of their business operations. Information technology has significantly ensured that businesses are coordinated more efficiently.

Nigerian organizations have not been left behind as a major number of organizations are increasingly adopting modern information technology systems.

The primary aim of conducting this study was to find out how the advent of information technology has impacted on operational processes in financial institutions. The research gears towards finding the extent to which information technology affects the occurrence of fraudulent practices in Nigerian banks.

Both primary and secondary data was used in this research work. The primary data was based on interaction between the researcher in an oral inter view with some employees of Broad Bank of Nigeria Ltd., while the secondary data was secured from journals, newspaper, magazines, the internet, textbooks and Broad bank data base.

The results of the study indicate that:

1. Information Technology has improved performance in customer service delivery by banks.

2. That computer fraud can be managed to the barest minimum.

3. That the advent of modern information technology has reduced the occurrence of fraud in banks.

In the light of the aforementioned, the following recommendations were made:

1. Banks should ensure adequate physical security to prevent accidental or intentional damage to the computer system and related equipment.

2. Ensure adequate techniques for maintaining transaction controls.

3. Tight security of software and data files to ensure programs is not tampered with.

4. Security communication networks to prevent unauthorized interception or alteration of electronic data.

5. To ensure that all possible measures are put in place such that the authorized users of the information technology system are individuals with integrity.

TABLE OF CONTENT

Title page

Declaration

Certification

Dedication

Acknowledgment

Table of content

CHAPTER ONE

1.0 Introduction

1.1 Nigerian Banking industry

1.2 Historical Background of Broad Bank of Nigeria Ltd.

1.3 Statement of the problem

1.4 Objective of the study

1.5 Hypothesis

1.6 Scope of the study

1.7 Significance of the study

1.8 Methodology of the study

1.9 Definition of Terms

CHAPTER TWO

2.0 Literature review

2.1 Concept of fraud

2.2 Theories of fraud

2.3 Effects of Fraud on banks

2.4 The emergence of on-line banking
2.5 The impact of information technology on fraud
2.6 The impact of fraud on public confidence in the banking system.

CHAPTER THREE

3.0 Research design and methodology
3.1 Introduction
3.2 Sources of data
3.3 Sampling technique and population
3.4 Sample size
3.5 Research Approach and strategy
3.6 Problems and limitation of study

CHAPTER FOUR: DATA ANALYSIS AND INTRODUCTION OF DATA

4.0 Introduction
4.1 Age range of Broad Bank workers
4.2 Educational background of bank workers
4.3 Marital status of Broad Bank workers
4.4 The ranks of bank staff involved in fraud
4.5 Magnitude of fraud in Nigerian Banks
4.6 Losses incurred as a result
4.7 Frequency of fraud by types
4.8 Analysis of fraud by person
4.9 Computer related fraud.
4.10 Major findings from hypothesis test

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATION

5.0 Summary

5.1 Conclusion

5.2 Recommendation

Bibliography

CHAPTER ONE

1.0 INTRODUCTION

Modern technology has taken the world by storm in recent decades. Particularly, the advent of the computer has completely revolutionized the way people live, work and play. Computers have affected businesses in numerous ways, allowing them to run more efficiently. However, there is a dark side to computers when individuals use them to lash out malicious assaults. These assaults may include fraud; identify theft, hacking, embezzlement and a wide array of other activities.

Fraud can be defined as all multifarious means which human ingenuity can devise, and which are resorted to by one individual to get on advantage over another by false suggestions or suppression of the truth. It includes all surprises, tricks, cunning or dissembling and any unfair way which another is cheated. Information fraud denotes any fraud committed through any of the information gadgets such as computers, telephone, fax e.t.c.

The declining level of business integrity in the banking industry may threaten the operations of the system in the post consolidation era. The volume of frauds and forgeries in Nigerian banks rose sharply by 107 cases (48 %) in the second quarter to 329, up from 222 in the previous quarter. The total amount involved in fraud and forgeries over the period was a whopping N1 .47bn, up by 25.6% from N 1.1 5bn in the first quarter of the year.

Whether simple or advanced, data analysis provides many benefits in the prevention and detection of fraud. While occupational fraud takes various forms, the result is always the same: the numbers generated by fraud cannot hold up to the unfailing logic of the accounting equation. For example, if executives add false sales and account receiveable to increase the organization's revenue, profits and cash will be out of the kilter. The advancement of technology has allowed this "accounting equation" to be systemized into computer logic and applied to company data. Results of this logic could take the form of a simple matching of the human resource file to the accounts payable vendor master file. On the other side of the coin, it could be an advanced neural network application focused on detecting money laundering schemes.

Computerization of banking operations enables the systematic transfer of all relevant information into the computer logic. This enables information to the accessed at the touch of a button. Transactions are also concluded on-line i.e. as soon customer approaches the bank for a transaction; it is executed and concluded on the spot. It has also greatly reduced the long queues and waiting time of carrying out business transactions in banks.

1.1 NIGERIAN BANKING INDUSTRY

The Nigerian Banking Act of 1969 term a bank as “any person who carried on banking business. The Act (as amended by section (1) (K) Banking Amendment Decree No. 3, 1970 stated that banking business of receiving monies from outside sources as deposits irrespective of the payment of interest and the granting of money, loan and acceptance of credits of the purchase of bills and cheques or the purchases and sales of securities for account of others or the incurring of obligation to acquire claims in respect of loans prior to their maturity or the assumption of guarantees on other warranties for others or the effecting of transfer, clearings such other transaction as the commissioner may on recommendation of the Central

Bank, by order published in the Federal Gazettes designate as banking business (Adekanye,1986).

1.2 HISTORICAL BACKGROUND OF BROAD BANK OF NIGERIA LIMITED (BBNL)

Broad Bank of Nigeria Limited was licensed to carry on commercial banking business in November, 1989. The bank formally commenced business on September, 3 1990 with mixed results until new core investors joined the bank (the AOG Group acquired a 55% stake). On acquisition, the new management, focused on the restructuring the business information technology and creating a niche market for the bank's product.

Broad Bank was restructured in October, 2001 and it has come from a negative net worth of N55mm in 2001 to N1.5bn core capital in 2004. The bank's authorized share capital at incorporation was N30,000,000.00 (Thirty Million Naira) divided into thirty million ordinary shares at N1 .00 each. This was increased to N50,000,000.00 in October, 1990 N150,000,000.00 in 1998 N1,000,000,000 in 2000 and subsequently to N2,000,000,000 (Two

Billion Naira) in 2001 of which N1,640,380,000 is wholly owned by Nigerians who have distinguished themselves

in various professions. With shareholders spread over 22 states of the federation. The bank is managed by a team of professionals with diverse experience in both domestic and international banking. The bank operates through a network of about 36 business offices strategically located all over Nigeria, and by virtue of its universal banking license, offers a complete range of financial services. The clientele base has access not only to commercial and consumer banking services, but also lease financing, equity and debt securities brokerage, transactions services, investment banking and advisory services. The bank has achieved market recognition through winning and successfully executing several high profile transaction mandates. In the last three years, the bank has continued to penetrate key economic sector, and today its client base includes major players in growth sectors such as Oil & Gas, Telecommunications and commerce. Innovation skillfulness and provision of customized financial solutions has been the cradle of the bank's success and these qualities have been instrumental to the achievement of their market position.

1.3 STATEMENT OF THE PROBLEM

Computer fraud is just one area of fraud which occurs in the banking industry, there are other types such as clearing fraud, cashiering fraud, forgeries of cheques and signatures, opening and operating of fraudulent accounts, over-invoicing for services to banks etc. but as the use of computer is gradually becoming indispensable in modern day banking, this research work becomes invaluable as this would profoundly prove useful to the banking industry.

1.4 OBJECTIVES OF THE STUDY

- To create an awareness of the impact of information technology in relation to banking services.
- To analyze the positive and negative contribution of information technology on banks.
- To identify the various areas of fraud associated with information technology in Nigerian banks particularly Broad Bank of Nigeria Ltd.
- To proffer recommendation on how these fraudsters/fraud could be checked.

1.5 HYPOTHESIS

These hypotheses are all stated in the null form and in such a way that testability and subsequent acceptance or rejection is easy.

HYPOTHESIS I

Hi — That the introduction of advanced information technology in Broad Bank of Nigeria Limited has improved performance.

Ho — That the introduction of advanced information technology in Broad Bank Of Nigeria Limited has not improved performance.

HYPOTHESIS II

Hi — That computer fraud in Broad Bank of Nigeria Limited can be curbed.
Ho — That computer fraud in Broad Bank of Nigeria Limited cannot be curbed.

HYPOTHESIS III

Hi — That the adoption of information technology has facilitated the increase of fraud.

Ho — That the adoption of information technology has not facilitated the increase of fraud.

1.6 SCOPE OF THE STUDY

The research topic is not beyond the confines of the impact of information technology in Broad Bank of Nigeria Limited. However the study is limited to the period from 2001 to 2004 to reflect when all the branches and processes in the BBNL were automated.

1.7 SIGNIFICANCE OF THE STUDY

The study is significant in that present and future researchers would access information on the impact of information technology on fraud in the banking industry.

The negative and positive impact of information technology will be of immense use to bankers, stakeholders as well as students of banking.

1.8 METHODOLOGY OF THE STUDY

Quantitative and qualitative methods of research were used in obtaining information. They include textbooks, journals, Broad Bank of Nigeria Limited publications, interviews etc.

1.9 DEFINITION OF TERMS

Fraud - Fraud includes a wide variety of acts all characterized by the intent to deceive the victim or to obtain unearned benefit.

Information Technology -The application of computer and telecommunication to manipulate information.

Analysis — Examination of issues by breaking it up into the parts of which it is made (Chamber Dictionary, 1980).

CHAPTER TWO

2.0 LITERATURE REVIEW

The encyclopedia Americana (volume 26), depicts that technology refers to ways of doing things; it explains that the term technology is derived from the Greek word technic meaning “art or craft”. The world book encyclopedia speaks about technology in the terms that it refers to all the ways people use their invention and discoveries to satisfy’ their need and desires.

Technology made a remarkable break through in the 18th century with the invention of the electric generator by Michael Faraday (1791-1867) and the telephone by Alexander Graham in 1875. These developments influenced the industrial revolution in Europe in the 18thcentury.

Technology, therefore involves scientific knowledge used in practical ways in industry, for example in designing new machines. Technology has affected business in numerous ways allowing them to run more efficiently and effectively. In banks for example, the advancement of technology has allowed for processes to be

systemized into computer logic and applied in carrying out transactions and enquiries. The entire banking operations are performed more efficiently and effective with a shorter turnaround time.

2.1 CONCEPT OF FRAUD

Fraud includes a wide variety of acts, all characterized by the intent to deceive the victim or to obtain an unearned benefit. The American Institute of Chartered public Accountants (AICPA) defines two basic categories of fraud; intentional misstatement of financial information, and theft. Other audit related agencies provide additional insight into the definition of fraud which can be summarized as follows:

Fraud consists of an intentional illegal act, the concealment of that act, and deriving a benefit from the act (Coderre, 1999).

Constructive fraud includes acts or words that tend to mislead others, e.g. when a sales person convinces a customer to purchase an automobile, house, electronic — etc.

Fraud can be committed not only by an individual employee, but also by a department division or branch within a company — or by outsiders. It can be directed against the organization as a whole or against parts of the organization. It can be the benefit of the organization as a whole, or of a part of the organization, or an individual within or outside the organization. Onuh (1982) explained that fraud in the banking system was the fourth factor which emphasized the need for a central note issuing body. In some countries, tow or more banks issue notes by the middle of the 19th century, over 1000 kinds of genuine banks notes were in circulation in the USA and over 5000 different kinds of fraudulent notes, the growth of counterfeit notes caused financial panic in the USA culminating in the passing of National Banking Act to restore financial sanity to the economy. Any bank granted a chatter under the National Banking Act was authorized to issue notes against billion deposits with the US federal Treasury or against certain government securities.

2.2 THEORIES OF FRAUD

The report on occupational fraud and abuse (Austine, ACFE, 1996) divides occupational fraud into three categories: misappropriation, corruption and fraudulent statements. Adewunmi (1986) in his explanation of fraud identified socio-economic lapses in society such as misplacement of societal values, the unquestioning attitude of society towards sources of wealth, the rising societal expectations from bank staff and the subsequent desire of the staff to live up to such expectations as contributory factors of fraud. Another theory states that banks have become persistent target of men of the under world mainly because banks are seen as the richest organization in any country.

Musa (1986) also opined that the main cause of fraud in Nigerian banks is traceable to general dishonesty in society. Since there is corruption in all facets of the Nigerian life, banks cannot be exceptions. He also mentioned other factors such as lack of call over system, lack of regular un-noticed rotation of clerks, doing more than one job which are incompatible.

There are some consequences on the causes of fraud in banks among authors, the degree to which they apply however differs from one organization to the other, under common law, there elements are required to prove fraud: a material false statement made with or intent to deceive (scienter), a victim's reliance on the statement on damages.

2.3 EFFECTS OF FRAUD ON BANKS

The obvious effects of fraud in the banking system includes: Loss of money belonging to the bank or customer which consequently affects the profitability of the banks because these monies have to be provided for. The loss usually results in reduced levels or resource availability which could hamper operations. This has a negative effect on the overall performance of the bank.

Others include loss of banks personnel in the case of armed robbery attacks, loss of confidence in the banking system which results in a setback in the patronage of the bank, job loss as some fraud cases are linked with carelessness on the part of the employees and that lead to their dismissal. In addition, fraud cases result in the distraction of management attention

increase in operating costs and wastage of time and resources on fraud prevention and other effects of fraud.

2.4 THE EMERGENCE OF ONLINE BANKING

According to Lawal (1992), since 1980, with the advent and widespread computerization of banking services, and innovation leading to the rise of large scale data transmission, network attempts have also been made to establish electronic payment system to overcome the limitation of the existing frame work dependant on postal system and telegraphic means of remitting funds.

The main technological device used in banking is the computer. The computer arrived on the banking scene in the early “1 960s”, then it was generally viewed by the banker as simply as a tool with the capacity to speed book keeping process. The real function of the computer was relegated to the background.

In a paper titled “computer delivery system”, Akinyola (1986) contended that the capacity activities of banks of industrialized nations with matching efficiencies could only have been made possible through the use of the

computer — a product of INFORMATION TECHNOLOGY. He said the low level of industrial performance

in developing countries suggested the inadequate use of computer and its technologies stressing that banking problems like delays, low volume of lending, limited services etc. could effectively be checked with the introduction of the computer.

With the third and fifth generation computers, banks began to realize the various applications of the computer processes. Technological advancements like the use of mobile phone, fax machine, electronic scanner/camera in banking were also recorded.

In recent times, there is an emergence of highly complex communication links regarded as the concept of connectivity. Banks have now adopted the use of specialized soft wares which allows the conclusion of transactions on the spot. These gadgets also allows the viewing and modifying of information in all the branches of the banks simultaneously, that is why banking in

Nigeria today allows a customer with an account domiciled in Zaria to be able to do transaction through that same account in Lagos. Some examples of the software include BASIS, Finnacle, and Globus etc.

2.5 THE IMPACT OF INFORMATION TECHNOLOGY ON FRAUD

Technology today has greatly influenced the flow of transactions in banks. It has ensured that all activities leave a trail that can be retraced when necessary. It has also ensured that the power to initiate and conclude a transaction does not rely on only one individual but that each step is handled by different individuals who operate with adequately protected passwords.

The on-going evolution of software provides auditors with an ever improving arsenal of tools and techniques while these tools were designed specifically for audit; they are equally adaptable to fraud detection and investigation and provide a virtually unlimited range of techniques for data interrogation. Through technology, banks easily analyze cash flow, rate of return, depreciation, balance sheet size, income etc.

In view of this however, the problem of information technology in relation to fraud now lies with human beings. One of the principles of using the computer depicts “garbage in garbage out”. Fraudulent operation can easily manipulate data and as a result of this losses are incurred. To this end, strict monitoring of the information technology systems must be ensured at all times.

2.6 THE IMPACT OF FRAUD ON PUBLIC CONFIDENCE IN THE BANKING SYSTEM

A major segment of the Nigerian populace do not have banking habit. This is largely due to illiteracy and partly the fact that banks are perceived as deposit mobilisers who fail to perform their responsibilities of balancing the savings surplus and savings deficit segments of the economy.

Fraud occurences also play a vital role in shaping the banking attitudes of the society. Prior to the pronouncement of the N25bn capital base requirement of the CBN, a lot of fraudulent activiries were abound in the system.

In some banks, an individual or group who has major shareholding could fraudulently take huge loans without adequate collateral. His inability to repay the loan results in distress situation which causes depositors to loose their monies. A great number of Nigerians have lost their monies in this situation in the distress banks like Savannah Bank, Allied Bank , City Express Bank etc.

These occurrences have greatly traumatised the populace as the NDIC insurance does not meet up to what they lost.

Other fraudulent activities that influence public confidence in the banking system include occurrences such as : unauthorised debits to customers` accounts, cheque forgeries, Armed robberies etc.

CHAPTER THREE

3.0 INTRODUCTION

The research approach and the strategy employed towards achieving the objective of this study is highlighted in this chapter.

3.1 SOURCES OF DATA

Both primary and secondary data were used in this research work.

Primary Data: - This was based on actual interaction between the researcher and some employees of Broad Bank of Nigeria Limited (BBNL) in a face to face interview session. This is to ensure that the researcher has first hand understanding of issues in the course of the research work. It has also helped in shaping the researchers opinion.

Secondary Data:- The sources of information consulted include journals, magazines, newspaper, textbooks, the internet etc.

3.2 SAMPLING TECHNIQUES AND POPULATION

All staff under the employment of Broad Bank of Nigeria Limited (BBNL) numbering 1580, constitute the population of the research being study.

The random sampling technique was adopted. Due to their common characteristics, every member of the research population stands an equal chance of being chosen.

3.3 SAMPLE SIZE

This include the cashier, branch manager, customer services manager, resident control officer, data center control officer, telephone, fax, computer etc (180 in number).

3.4 RESEARCH APPROACH AND STRATEGY

The research approach adopted in this study has being the qualitative and quantitative approach.

For reference purposes, textbooks, journals, newspapers, magazine, in-house publications, internet were consulted. ,in addition, due to the fact that the researcher is currently a staff of Broad Bank of Nigeria limited (BBNL),

she had easy assess to the members of staff and had unstructured interview sessions with them individually as well as in group interactive forums.

The researcher also conducted interviews with some staff of CBN, NDIC, as well as members of the general public.

3.5 PROBLEMS AND LIMITATION OF THE STUDY

The research relies heavily on secondary data as such the incidence of deliberate distortion of facts to suit the researchers' desired requirement may occur.

Secondly, the fact that the researcher is a staff under the employ of the organization under review constituted a hindrance as the people being interviewed were being deliberately evasive contending that the interviewer could source for information her self since she is part of the organization.

Thirdly, due to time constraint, this research, particularly the face to face interview was limited to Abuja metropolis.

Fourthly, due to the nature of work in this organization, the interview sessions were constantly interrupted by office engagements.

Fifthly, information relating to the study under review was not easily gotten due to nature of strict safeguarding of information and data in banks. Data was mostly restricted and staff were reluctant to say much and were also not disposed to filling out questionnaires. Irrespective of the above, data were

collected, analyzed and the result of analysis and the inferences drawn from them are exhibited in the next chapter.

CHAPTER FOUR

4.0 INTRODUCTION

Data gathered will essentially be summarized in the form of frequency distribution table while simple percentage method will also be utilized.

A total of 60 members of staff of Broad Bank of Nigeria limited (BBNL) were interviewed based on simple random system. This chapter will be based on the analysis of the responses of the 60 respondents, data collected from Broad Bank of Nigeria limited (BBNL) inspection unit, NDIC and CBN journals as well as responses from some of their staff.

Table 4.1

AGE RANGE OF BBNL WORKERS

AGE RANGE	NUMBER OF RESPONDENTS	PERCENTAGE
21-30 years	25	41.7%
31-40 years	30	50%
41-50 years	5	8.3%
Total	60	100%

Source: Response of 60 BBNL respondents.

The analysis shows that the majority of BBNL workers range between the ages of 31-40. There are 30 respondents in this group represented by 50% of the entire population.

25 respondents are between the ages of 21-30 years old, represented by 41.7% of the entire population. While those within the age of 41-50 years old are five in number represented by 8.3% of the entire population of respondents. This shows that majority of the workers have attained a level of experience which could be manipulated to defraud the organization.

Table 4.2

EDUCATIONAL BACKGROUND OF BBNL WORKERS

QUALIFICATION	NUMBER OF RESPONDENTS	PERCENTAGE
HND/DEGREE	39	65%
OND/NCE	15	25%
SSCE	4	6.7%
PLSE	2	3.3%
Total	60	100%

Source: Response of BBNL Respondents.

The data shows that those who attended the university and polytechnic make up the highest percentage, 39 of the respondents represented by 65% of the total number of the population make up this group. Those who posses Ordinary National Diploma and NCE Certificate follow with 15 respondents represented by 25% of total number of population. The primary and secondary school certificate holders have 4 and 2 respondents representing 6.7% and 3.3% respectively.

This shows that majority of the staff have adequate qualification and as a result of that, the capacity to improve and sustain their performance on the job and ensure top quality relationship management of their customers.

Table 4.3

MARITAL STATUS ON BANK WORKERS

MARITAL STATUS	NUMBER OF RESPONDENTS	PERCENTAGE
Married	**35**	**58.3%**
Single	**25**	**41.7%**
Divorce (widowed)	**0**	**0%**
Total	**60**	**100%**

35 respondents are married representing 58.3% of the total population. The single respondents are 25 representing 41.7%, while there are no divorced or windowed respondents.

This analysis shows that majority of the staff have families to cater for and such are responsible.

Table 4.4.

RANKS OF BANK STAFF INVOLVED IN FRAUD

RANK	2001		2002		2003	
	Number	%	Number	%	Number	%
Supervisors & Managers	55	36.18	16	18.80	25	23.58
Officers, Accountants & Executive Assistants	60	39.47	48	56.50	41	38.68
Clerks and cashiers	30	19.74	13	-	25	23.58
Typists, technicians and Stenographers	0	0	0	0	0	0
Messengers, Drivers, Cleaners, Security Guards & Stewards	5	3.29	4	4.7	7	6.60
Temporary Staff	2	1.32	4	4.7	8	7.55
Uncategorized Staff	0	0	0	0	0	0
Total	152	100	85	100	106	100

(Source: Banks Returns (NDIC 2003 Annual Report and Statement of Accounts)

The table shows the rank and number of banks' staff involved in frauds and forgeries during the year and previous two years. A total of 106 staff of banks were reported to be involved in frauds and forgeries in 2003, an increase of about 24.7% when compared with the pervious year's level. That means that higher number of staff perpetrated fraud and forgeries involving considerably higher amounts than in the previous years. Of the total, core operations staff such as supervisors officers, accountants, managers, executive assistants, clerks and cashiers accounted for about 85.84 %, a decrease of 4.8 percentage points relative to the previous two years' levels.

Table 4.5

MAGNITUDE OF FRAUD IN NIGERIAN BANKS

INDUSTRY WIDE

JANUARY- DECEMBER 2002 JANUARY- DECEMBER, 2003 JANUARY- DECEMBER 2004

ATTEMPTED	ACTUAL	ATTEMPTED	ACTUAL	ATTEMPTED	ACTUAL
125,657,562.49	57,103,501.05	113,_249,565.08	23,034,149.57	19,736.597.64	1,200,000.00

(Culled from CBN Consolidation Report on Fraud and Forgeries to Committee of Chief inspectors - May 28, 2004)

*** Please find Broad Bank data (sorted from the most recent) on the next page.**

BROAD BANK (SORTED FROM MOST RECENT FIRST)

No	Fraud date	Description	Amt involved (N)	Actual loss (N)	Rank of staff involved
1.	30/09/05	Lodgement of stolen dividend warrants.	42,710.40	-	-
2.	26/04/05	Lodgement of cloned cheques	5,574,250.00	5,574,250.00	-
3.	10/10/03	Diversion of customer's deposit	150,000.00	-	IT
4.	30/04/03	Fraudulent credit of salaries into a staff 's account.	1,998,042.51	-	B O
5.	25/02/03	Theft of a customer's cash deposit	1,345,000.00	-	TBO
6.	20/11/02	Fraudulent withdrawals from five branches via- forged inter branch vouchers.	13,450,000.00	13,450,000.00	-
7.	06/02/01, 09/02/01, 27/12/01	Used inter branch vouchers to make cash withdrawals with out prior deposit.	1,645,000.00	1,645,000.00	BO, Clerk
8.	04/09/01	Manipulation of inter branch account in favour of a customer.	75,350,146.00	75,350,146.00	AM, Officer II
9.	02/04/02	Granting of unauthorized credit facility	18,000,000.00	-	AM
10.	25/05/01	Conversion of VAT cheques	1,538,497.99	1,538,497.99	Officer 1
11.	20/06/01	Falsification of clearing schedule.	68,000,000.00	-	Dispatch rider

In any discussion of Fraud, the amount involved is of high interest. The amount involved as well as the amount lost to the bank often form the nucleus of the analysis. The amount involved denotes the total sum targeted by the fraudsters, while the amount actually lost to the bank is defined as the amount actually withdraw an carted away by the fraudsters.

The table shows that between January to December 2002, ₦57,103,501.05 is the actual amount lost as a result of fraud in Nigerian banks while ₦125,697,562.49 is the total amount attempted. In 2003, the actual amount lost drastically drop to ₦23,034,149.57 as against ₦ 113,249,565.08 attempted. Between January and April 2004 the amount lost stood ₦1,200,000.00 while attempts totaled ₦ 19,736,597.64.

4.6 LOSSES INCURRED AS A RESULT OF FRAUD

Please refer to Table 4.5.

The effectiveness of the various apparatus for the detecting and stemming fraud in bank can be measured by the difference between amount involved and the total lost to banks and customers. This shows the level of investment and expertise committed to managing fraud in the organization and is of vital importance.

Table 4.7

FREQUENCY OF FRAUD BY TYPES

No	Type of fraud	Total No Of cases reported	Involving bank personnel only	Involving outside personnel only	Not specified	Amount involved (₦)	Expected loss (₦)
1.	Cashiering fraud	3	3	-	-	570,360.89	272,965.00
2.	Falsification of account	11	5	5	-	10,504,740.00	1,712,740.00
3.	Forged cheques with forged signatures	58	9	42	7	189,054,679.34	37,328,695.79
4.	Illegal printing of bank document	3	-	2	-	45,025,362.08	-
5.	Clearing fraud	6	4	2	-	67,573,698.83	119,404,433.97
6.	Computer fraud	1	1	-	-	183,900.00	-
7.	Telex frauds	3	0	2	1	56,496,016.40	-
8	Foreign exchange frauds	4	4	-	-	11,365,893.37	6,650,000.00
9	Cross firing and cheques kiting	1	1	-	-	432,000,000.00	432,000,000.00
10	Cash theft/suppression	63	57	5	1	1,335,339,697.28	132,865,038.21
11	Opening and operating fraudulent accounts.	12	4	8	-	38,061,761.67	6,761,822.14
12	Over-invoicing for services banks	2	2	-	-	1,950,000.00	1,950,000.00
13	Armed robberies	16	-	15	1	69,255,701.58	69,255,701.58
14	Ficticious bank branches	-	-	-	-	-	-
15	Miscellaneous frauds	21	8	9	4	48,991,017.01	33,643,420.80
16	Fraudulent withdrawals	79	23	45	3	113,883,191.12	33,561,935.69
	TOTAL	283	121	135	18	2,417,316,519.57	875,407,253.21

(Sources: Fraud and Forgeries in Nigerian Banking Industry (3rd Quarter 2004) –FINANCIAL INSTITUTIONS TRAINING CENTER-6th September 2004.

The analysis shows fraudulent withdrawal as the fraud type with the highest number of cases, 79 with an expected loss of N33,561,935.69 this is follow -

ed by cash theft/suppression which recorded 63 cases with an expected loss of N37,328,695.79. Computer related fraud recorded only one case with no expected loss. Others include over-invoicing of service to bank, cashiering fraud, cheques firing and check kiting.

4.8 ANALYSIS OF FRAUD BY PERSONS

Please refer to table 4.4.

This shows that members of top management and middle management which include supervisors, managers, officers, accountant and executive assistants constitute a greater percentage of persons involved in fraud in banks.

In the year 2000, clerks and cashiers were 27.8%, while supervisors and managers represented 26.8% of the population. Officers, accountant and executive assistants constituted 20.5% while the remaining was shared among other categories of staff as demonstrated in table 4.4.

In 2001 officers, accountants and executive assistant constituted 39.47% of the population followed by supervisors and managers represented 36.18 of the population. Clerks and cashiers stood at 19.74%.

The year 2002 however recorded a whopping 56.5% representing officers, accountants and executive assistants, while supervisor and managers stood at 18.8%. Clerks and Cashiers represented 15.3% of the population.

4.9 COMPUTER RELATED FRAUD

Please refer to table 4.7.

Table 4.7 shows that computer related fraud accounts for one of the least fraud types recorded in the period under review. The methods in which the computer could be used in fraudulent practices include- file manipulation, input manipulation, operation manipulation and program manipulation.

The computer is the backbone of information technology in banks. Its "garbage in garbage out" principle makes the system vulnerable as any person can decide to feed in what ever data to defraud an organization.

This issue is however address by most of the modern Information Technology systems used in banks today. These systems do not allow only one user to carry out any particular transaction from start to finish. Transaction are usually first initiated by one user whose input has to be verified by second user and finally authorized by a third party before conclusion. All these users usually have password which they are bound by an oath of secrecy to keep only to themselves. This whole process ensures a check and balance situation which makes it difficult for any individual to defraud the bank.

Apart from password secrecy, the computer terminal rooms are strictly monitored to ensure that no one person is alone in the terminal room at any point in time. Modern cameras are also fitted for surveillance.

Information technology through the use of computers as ensured improved turn around time on transactions. Customers can now carry out their transactions in good time unlike the days of manual banking with attendant long queues and archaic processes. In BBNL particularly, improved turn

around time means much more transactions are carry out within a such period and this translate to greater profit margins.

Computer place a vital role in globalization which targets the world becoming one global village in which business dealings are carried out with the greatest ease. Western Union Money Transfer, Master card payment system, value cards, ATMs are all product of modern information technology in financial institutions.

4.10 MAJOR FINDINGS OF THE HYPOTHESES TEST

HYPOTHESIS ONE

H1- That the introduction of advance information technology in Broad Bank of Nigeria Limited has improved performance.

H0 – That the introduction of advanced information technology in Broad Bank of Nigeria Limited has not improved performance.

The staff management and customers of BBLL agree that the introduction of advanced information technology has greatly improved the performance of the bank customer service delivery and the public perception of the bank thereby increasing patronage. Therefore, the hypothesis is null and the alternative is rejected.

HYPOTHESIS TWO

H1- That computer fraud in BBNL can be curbed.

H0 – That computer fraud in BBNL cannot be curbed.

A review of the data collection from the Inspection unit and interview with some staff selected of random clearly shows that computer fraud in BBNL can be managed to the barest minimum in order to give confidence to the public as to the safety of their deposits.

The hypothesis is therefore null thus rejecting the alternative hypothesis.

HYPOTHESIS THREE

H1 – That the adoption of modern information technology has facilitated the increase in fraud.

Ho – That the adoption of modern information technology has not facilitated the increase in fraud.

A review of the results of the interview and data collected from the BBNL Inspection unit shows that due to the various measures put in place to ensure constant checks and balances on every transaction, fraud in banks has been on the decrease.

We therefore reject the null hypothesis and confirm the alternative hypothesis.

CHAPTER FIVE

5.0 SUMMARY

A relatively small number of highly events involving loss or near loss from fraud have created an impression that eletronic payments are less secure than equivalent paper- based processing systems. Computer error or computer fraud tends to be similar in kind to non-computer error or fraud, but uses the computer`s inherent characteristics, such as speed or anonimity, to complete an illegal transaction. Unlike human a computer can be expected to run through the same set of of tasks every time a process is completed, without changing its judgement and without forgetting any step the computer will exactly allocate the amount of freshness and attention to checking the millionth transaction as it did to checking the first.

The principles behind the design of a secure electronic system are the same as the principles behind the achievement of any secure treasury arrangement, manual or computerised. By idetifying the requirements for adequate security, it should be possible to use the inherent displine of computers to design and implement an electronic system which is secure at the time of its design; neverthe less, the perfect solution may be prohibitively expensive.

5.1 CONCLUSION

Computers can increase productivity and efficiency within a financial institution or they can be used to commit fraud and cause substantial financial loss. Therefore, computer crime in financial institutions is an increasing concern because computer processing can circumvent traditional security and control techniques. Particular security concerns result from the prolifiration of microcomputer, local area networking, and on-line system that allow more access to the mainframe computer.

Computer fraud is certainly not new and does not necessarily involve the use of microcomputer. Computer fraudsters even if caught are not prosecuted in many cases. As a result, the problem of white-collar computer fraud cases is never reported because of embarrassment, loss of public confidence, false arrest concerns, and the overall difficulty of prosecution.

Compromising the computer system in a financial institution can occur from an outside intruder using a public telephone network connected to the computer, or an employee or unauthorised person within the organisation using a terminal or microcomputer. This is because outside electronic penetration depends on the use of telephone lines with dial-up capability, financial institutions that do not have communication lines connected to the computer are not at risk from hackers. However, financial institutions are certainly not immune to fraud, since penetration from within is the most likely means of gaining access to sensitive computer data. Thus the vast majority of computer fraud is carried out by trusted employees.

Financial institutions BBNL not an exception are heavily dependent on automated systems and electronic funds transfer network for various business activities. As a result financial institutions are exposed to the possibility of significant fraud in the computer area because:

- Computer records are in electronic form.
- Transaction may be initiated from remote facilities by various employees, customers and external parties.

- Computer processing of accounts and transactions data may be performed by a group of personnel external to the financial institutions (e. g. service providers).

5.2 RECOMMENDATION

The nature of computer fraud is such that a financial institution without adequate internal control and security could experience substantial losses that remain undetected for a long time. They should be concerned with both computer and electronic transactions security issues. Thinking that it can only happen to others can increase risk and potentially weaken existing security and control precautions. Therefore maintaining the security of a computer system and electronic transactions should involve:

- Adequate physical security to prevent accidental or intentional damage to the computer system and related equipment.
- Software and data files security to ensure that computer programs and data files are not altered accidentally or deliberately.

- Techniques for maintaining transaction data controls and for analysing the reasonableness of transactions to detect and report possible crime attempts.
- Use of customer identification methods to preclude unauthorised individuals from initiating transactions to customer accounts.
- Security communication networks to prevent unauthorised interception or alteration of electronic data.
- Adequate internal controls to prevent, detect and correct computer fraud and other concerns.

BIBLIOGRAPHY

Adekanye, F. (1986) "Fraud in Banking Transaction" The Nigerian Bankers, Vol. 6 No. 1 Nigeria Chartered Institute to Bankers, Lagos. Land Mark Publication Ltd., Lagos.

Adewunmi, W. (1986) Fraud in Banks, an overview in Wole Adewunmi (Ed) Fraud in Banks (Nigerian Chartered Institute of Barkers, Lagos). Land Mark Publication Ltd. Lagos.

Broad Bank of Nig. Ltd. Fraud Data Base (Inspection Unit)

Central Bank of Nig. (2004) Consolidation Report on Fraud and Forgeries to Committee of Chief Inspectors (May 28th 2004).

David G.Coderre (1999) Fraud Detection using data analysis and Techniques to detect fraud.

Darek & Heather S.A (1983) Dictionary of Management, 2nd Edition Grawther publishing Company Ltd.

Edhodaghe J. U. (1991) "Frauds Forgeries in the Nigerian Banking Industry being a paper presented at a seminar (Nigerian Chartered Institute of Bankers, Lagos).

Financial Institution Training center (2004) Fraud and Forgeries in Nigeria Banking Industry (6th September 2004).

Harold kowntz & Cyril O. Donnel (1974) " Essential of Management" New York McGraw Hill, chapter 3.

Isaac Charles (1994) "The impact of technology in banking" First Bank of Nigeria Plc. Bi-annual Review PP. 52-55.

Information Systems Control Journal Vol. 3,2004

National Deposit Insurance Cooperation 2002 Annual Report & statement of accounts.

Oliver & Chapman (1993) "Data Processing and Information Technology"