CORPORATE FRAUD CONTROL AND PREVENTION SYSTEMS IN COMMERCIAL BANKS IN ENUGU STATE, NIGERIA

BY

UGWOKE, ERNEST O.
PG/Ph.D/05/39896

A THESIS SUBMITTED TO THE DEPARTMENT OF VOCATIONAL TEACHER EDUCATION IN FULFILLMENT OF THE REQUIREMENTS OF THE AWARD FOR THE DEGREE OF DOCTOR OF PHILOSOPHY (Ph.D) IN BUSINESS EDUCATION

March, 2010

APPROVAL PAGE

This thesis has been approved for the Department of Vocational Teacher Education (Business Education), University of Nigeria, Nsukka.

By

_____	_____
Prof. E. C. Osuala	**Internal Examiner**
Thesis Supervisor	
_____	_____
External Examiner	**Dr. E. E. Agomuo**
	Head of Department

_____

Prof. G. C. Offorma

Dean, Faculty of Education

CERTIFICATION

It is hereby certified that Ugwoke, Ernest O., a Postgraduate student in the Department of Vocational Teacher Education, with Registration Number PG/Ph.D/05/39896 has satisfactorily completed the requirements for research work for the award of the Degree of Doctor of Philosophy (Ph.D) in Business Education.

The work embodied in this thesis is original and has not been submitted in part or full for any other diploma or Degree of this or any other University.

_____ _____

Ugwoke, Ernest O. (Student)

Prof. E. C. Osuala (Thesis Supervisor)

DEDICATION

This research work is dedicated to the Almighty God for His infinite mercies, guidance and blessings throughout the study.

ACKNOWLEDGEMENTS

The researcher thanks God for guiding him through this study. He is grateful to his Supervisor Prof. E. C. Osuala for his constructive criticisms and guidance on the study. He is also grateful to Prof. C. A. Obi, Prof. C. Oreh, Dr.

E. E. Agomuo, Dr. E. A. C. Etonyeaku, Dr. F. A. Okwor, Dr. R. O. Mamah, Dr. E. C. Osinem, Dr. V. N. Nwachukwu and Dr. K. O. Usman for their constructive suggestions that helped to sharpen the focus of this study. The researcher is equally grateful to other lecturers in the Department of Vocational Teacher Education, University of Nigeria, Nsukka who contributed to the successful completion of this thesis. The researcher wishes to express his sincere thanks to the Managers, Accountants and Supervisors of the commercial bank branches operating in Enugu State for their contributions that led to the successful completion of this study. His sincere thanks also go to the Managers, Accountants and Supervisors of the 10 commercial banks in Ebonyi State where the research instrument was pre-tested.

Finally, the researcher remains indebted to members of his nuclear family for their understanding and cooperation with him even when he deprived them of his usually fatherly comfort, especially his wife, Ugwoke Cordelia Chinasa who wholeheartedly encouraged him to go on for the programme and assured him of her full assistance in the proper care of the family. The researcher also thanks the following for their contributions towards the success of this study: Godwin Nwodo, Nwora Nwodo, Mr. J. K. Edeh, Elder Chim Nwokocha and others too numerous to mention.

Ugwoke, Ernest O.

TABLE OF CONTENTS

APPENDIX

LIST OF TABLES

ABSTRACT

The major purpose of the study was to determine the corporate fraud control and prevention systems in commercial banks in Enugu State of Nigeria. The study adopted a survey research design. Eight research questions were answered while five hypotheses were tested at 0.05 level of significance. The population of the study comprised 288 management staff in the 96 commercial bank branches operating in Enugu State. The entire population was studied. Structured questionnaire containing 97 items was used for the study. The questionnaire was subjected to face validation by experts. The questionnaire was pre-tested on 30 management staff in 10 commercial bank branches in Ebonyi State of Nigeria. Kuder-Richardson (K-R20) Reliability Coefficient of 0.96 and 0.99 were obtained for questionnaire items in sections B and C of the questionnaire respectively while Cronbach Alpha Reliability Coefficient of 0.99, 0.98, 0.98, 0.99, 0.99 and 0.98 were obtained respectively for the other six clusters in sections D to I. The questionnaire was administered personally by the researcher with the help of two trained research assistants. The research questions were answered using frequencies and percentages for research question one and two while mean and standard deviations were used for answering research question three to eight. The five null hypotheses were tested at 0.05 level of significance using t–test statistic. The problem of the study was that the corporate fraud control and prevention systems might not be adequately available, utilized and effective in controlling and preventing fraudulent activities in the commercial banks. However, it was found and concluded that most of the corporate fraud control and prevention systems were available and utilized most times in the commercial banks and they were effective in controlling and preventing fraudulent activities in the banks. The

commercial banks encountered many problems in the utilization of the corporate fraud control and prevention systems but many strategies for enhancing the effective utilization of the systems were identified. The result of the study would be used by Accounting Educators for guiding and counseling the management of commercial banks, bank customers, investors and other stakeholders of commercial banks especially for fraud control and prevention. It was recommended that the management of the commercial banks should regularly review and update the systems to ensure that they are relevant, adequate and effectively utilized. The management of commercial banks should also endeavour to ameliorate the identified problems encountered in the utilization of the corporate fraud control and prevention systems with the necessary strategies.

CHAPTER ONE
INTRODUCTION

Background of the Study

Commercial banks are corporate financial institutions that accept monetary deposits from customers and effect withdrawals upon demand by the depositors. Commercial banks like every corporate institution are registered under the company and Allied Matters Act (CAMA) of 1959 and 1990 as amended. Commercial banks play a central role in the domestic and international financial system of an economy. One of the intermediate roles of commercial banks is to ensure that capital is allocated in an efficient manner to facilitate growth and development in the economy through savings, investments and lending of credits to customers. Commercial banks provide the mechanism for settling personal and business transactions including fund transfers for both domestic and international trade. Commercial banks, therefore, represent an important nerve centre of an economy, which controls and lubricates its operation via an effective implementation of the monetary policies initiated by the Central Bank of Nigeria.

Commercial bank activities in Nigeria, according to Aigbokhaevbolo (2001), started in 1892 with the establishment of the African Banking Corporation by the British West Africa. The bank was later known as the Standard Bank Ltd, which is now called First Bank of Nigeria PLC. This was followed by the establishment of the Barclays Bank Ltd. (now Union Bank of Nigeria PLC) in 1917. Since then, the number of commercial banks in Nigeria has increased. According to the Central Bank of Nigeria Report (2006), 89 Commercial banks operated in Nigeria prior to the conclusion of the banking

industry consolidation exercise in December, 2005. However, only 25 of them survived the consolidation exercise, although some of the banks have merged since then e.g. IBTC and Stanbic banks. The consolidation exercise was the recent regulation on the capitalization of commercial banks to a minimum of N25 billion in Nigeria.

Commercial banks operating in Nigeria fall into two categories: the old and new generation banks. According to Ekine (2008), Nigerian commercial banks are mainly classified into old and new generation banks. He stated that the old generation banks are distinguished from the new generation banks by age, rural banking activities and their general method of operations. Ekine further stated that the old generation commercial banks are more conservative in their operations than the new generation banks, even though all the banks have adopted computerization and the use of electronic on-line banking services. The above assertion is in line with Agu (2008) that old generation commercial banks of the Nigerian banking sector are still greater labour intensive in their operations despite the current age of computerization and Internet banking. StanbicIBTC Bank in a special Report (2008) stated that the old generation banks were those few highly regulated banks mostly controlled by government before the introduction of the Structural Adjustment Programme (SAP) in 1986. It was also stated in the Report that with the reduction and privatization of government shareholding in banks which arose from the Structural Adjustment Programme new commercial banks categorized as the new generation banks were established. The old generation commercial banks, according to the Report, are those commercial banks that have fully embraced the rural banking operation policy of the federal government

introduced in 1976.The old generation commercial banks have many of their branches in rural towns and communities all over the country; a practice which is still strange to the new generation banks in Nigeria. The StanbicIBTC Bank Special Report also stated that the old generation banks are the likes of First Bank, Union Bank, UBA and Afribank.

The development in information and communication technology (ICT) has changed the profile of commercial banks in Nigeria. The huge investments in information and communication technology by the banks show their desire to function on a comprehensive electronic platform. The banks have adopted many electronic and on–line banking products for their services. Some of the products are Automated Teller Machine (ATM), Electronic Point-of-Sale (POS) Terminal services, Internet-banking (i-banking) and mobile banking services which are SMS-Based. These products make use of various forms of electronic cards. According to Ogbulie (2007), the application of information and communication technology products has become the dominant issue in commercial banking in Nigeria. The introduction of the on-line and electronic real-time banking services has resulted in new payment systems and fund transfers that give the banking customers the needed satisfaction in modern banking. However, he stated that those products are often threatened by frauds.

Achaka (2004) defined fraud as an action of dishonesty, deceit, false claims, unlawful possession and dispossession of money, goods and services thereby causing the other party to be at disadvantage. Frauds can occur to individuals and also to business organizations including commercial banks. Fraudulent activities that occur in business environments are called corporate frauds. Corporate frauds are criminal activities in business organizations

targeted to diminish by misappropriation, misrepresentation and manipulation the assets, revenues and profits of the organization. Ochejele (2004) defined corporate frauds as a deliberate step taken by one or more individuals who may be internal or external to a business organization, to deceive or mislead the organization with the objective of taking an unfair advantage of money, goods and services. Common corporate frauds are embezzlement, payment against uncleared cheques and unauthorized lending.

Corporate frauds can be committed by the persons in management, the employees of a business organization and people external to the organization. Sometimes it is committed by a collaboration of the employees with external parties. Corporate frauds most times portray a betrayal of trust and a breach of the core fabric of the working and personal relationships in a business environment. Corporate frauds have become more advanced, complex and devastating in recent years with the emergence of sophisticated systems associated with the great advances in Information and Communication Technology (ICT). Ochejele (2004) stated that the incidence of corporate frauds in the Nigerian banking system has become even more pronounced in this era of increasing globalization of the financial markets and other economic institutions. Aderinokun (2007) stated that Nigerian commercial banks lose billions of naira every year because of various forms of fraudulent activities. He stated that commercial banks in Nigeria lost more than N48 billion between 2001 and 2006 because of the increasing incidence of fraudulent activities in banks. Nigeria Deposit Insurance Corporation (NDIC) Report (2007) in support stated that the number of fraud cases in Nigerian banks grew from 1193 in 2006 to 1553 in 2007 involving N4.83 billion and N10.05 billion respectively.

The Report listed the causes of bank frauds as follows: poor accounting system, weak internal control, and inefficient supervision of subordinates, uncompetitive remuneration and perceived inequality in reward as well as disregard of know-your-customer (KYC) policies.

Commercial banks are adversely affected by frauds because of the huge financial assets handled by them. The computerization of banking and the use of electronic banking services also aid fraudulent activities in banking environment by making perpetration easy and fast. Ovuakporie (1998) identified different forms of bank frauds, which include payment against uncleared cheques, unauthorized lending and borrowing, impersonation, cloning of cheques and money laundering. Ovuakprie stated that the banks are affected by many electronic frauds owing to the use of the Internet and other computerized devices. According to the author, newer forms of fraud that use the advantage of technological progress have also developed. These include: Unauthorized Automated Clearing House (ACH) draft, multiple electronic deposits of the same cheque and electronic intra bank transfer. Commercial banks are usually equipped with corporate fraud control and prevention systems to reduce the prevalence of fraudulent activities. Corporate fraud control and prevention systems are established to ensure that bank assets and transactions are secured. Corporate fraud control in particular is the restraint, authority, command, regulation and a check on the activities of an organization. It is to ensure that the objectives of the organization are met. It is the means of operating, regulating, directing and testing the activities of the organization that establishes them. Onah (2003) stated that control defines the power and authority of an organization to direct, order or restrain the activities and

conduct of people, internal and external, with a view to ensuring their conformity with organizational plans and objectives. The author further stated that control focuses on the ability of the organization to determine and effectuate its intentions using its human resources. Control describes all the organizational efforts to ensure that employees, customers, investors and other parties' behaviours are in line with the organizational plans and standards. After the organizational standards and plans have been set, control represents the organizational efforts to ensure the people's compliance with those standards. Fraud control, therefore, means the measurement and correction of performance activities in order to ensure that enterprise objectives and plans devised to attain them are being accomplished. It consists of verifying, checking and regulating to ensure that everything occurs in conformity with the plans adopted, the instructions issued and the principles established.

Corporate fraud prevention systems are the series of physical, logical and procedural barriers established by an organization to discourage the incidence of fraudulent activities in the organization. The aim of a fraud prevention system is to hinder, to stop or to make impossible the occurrence of fraudulent activities in an organization. The Chambers Dictionary (2006) described prevention as an action of stopping someone from doing something or stopping something from happening. It stated that prevention is the strategy established for the avoidance or preclusion of something by care, forethought or obstruction. Fraud prevention systems are, therefore, installed to stop people from committing fraud or to stop fraud from occurring in the first place. According to the bank of Netherlands (2006), fraud prevention systems are designed to ensure that events, which threaten operations in an organisation, for

example a commercial bank, do not occur or occur infrequently. The bank stated that careful designing and locating of computer centers and other security devices to stop unauthorized access to assets and systems in the organisation are aspects of fraud prevention.

Adequate investment in fraud control and prevention systems strengthens commercial banks' defences against any form of fraudulent activity. Regularly maintained fraud control and prevention systems also ensure that most corporate frauds are minimized. According to Usman (2004), frauds may not be totally eliminated though there are control and preventive measures that can drastically reduce the amount of frauds in a business. Such measures, according to him, include adequate physical and electronic security, pre–employment screening, installation of surveillance equipment, etc. The author further stated that organizations that seek those measures are successful while those that ignore them lose heavily.

Most commercial banks, according to Vital (1999) have control facilities and measures designed to assist in the prevention of fraudulent activities. However, Vital regretted that some of them are not utilized extensively to curb fraud menace. The extent to which they are utilized determines their success in fraud control and prevention. The extent of utilization of the systems available, therefore, needs to be ascertained for effective fraud control and prevention. Akwaja (2007) supporting the view stated that the utilization of the fraud prevention measures in banks is still low. He stated that Nigerian commercial banks have lost heavily in the past few years to fraud prevention measures that were not properly implemented.

The fraud control and prevention systems utilized in commercial banks should be effective. Onah (2003) defined effectiveness as the degree of success expected from a chosen procedure or method. He stated that effectiveness is a function of the adequacy of the methods and procedures. According to Osuala (2004), effectiveness is the ability to do the right thing to achieve the goal of a business. Effective fraud control and prevention systems can reduce fraudulent activities with minimum expense, waste and effort. They should be cost-effective to the organisations that establish and utilize them. The degree to which the available fraud control and prevention systems minimize the incidence of fraudulent activities is based on their effectiveness. However, Charlton and Taylor (2004) stated that the effectiveness of the fraud prevention systems in financial institutions including commercial banks has not yet been ascertained.

Most commercial banks encounter some problems in the establishment and implementation of fraud control and prevention systems. These problems emanate from poor infrastructure, lack of finance, unskilled manpower and complexity of operations. Ojuri (2007) stated that the banks encounter the problems of high costs of acquisition and maintenance of systems. They also suffer from the problems of complex programme application, network and power disruption, and shortage of skilled personnel to operate the complex systems.

Commercial banks have always strived to improve their fraud control and prevention strategies. However, Shackell (2000) stated that as the responses of the commercial banks become more successful so the fraudsters have become more creative by evolving new and more deadly methods of

frauds. Shackell (2000) stated that corporate fraud is an undeniable fact of business life, affecting businesses, large or small. Shackell further stated that as the systems and technologies are further developed, the perpetrators of corporate frauds tend to become bolder and more advanced in their crimes, thus forcing organizations to evolve new techniques for averting the newer forms of fraudulent activities. It is therefore imperative on commercial banks to seek ways of improving their fraud defences and to counteract any problems they experience in the establishment and utilization of the systems. Current firewall technologies like data encryption, passwords, personal identification, etc are, therefore, the imperatives for banks.

KPMG (2006) stated that corporate organisations continuously strive to achieve compliance with an array of new anti-fraud laws and regulations that are prescriptive on the design of controls and prevention strategies against corporate fraud and misconduct. KPMG also stated that it is the responsibility of the management of an organisation to understand the fraud and misconduct risks that can undermine the business objectives. KPMG further stated that it is also the responsibility of management to determine the anti-fraud programmes utilized against fraud and misconduct in the organisation. The focus of management, according to KPMG, is also to gain insight on better ways to design or evaluate controls to prevent, detect and respond appropriately to fraud and misconduct. Other responsibilities of management as it concerns corporate frauds and misconducts are to create sustainable processes and structures for managing fraud risks and for improving performance in the organisation. Furthermore, KPMG stated that it is also the duty of management

of any organisation to strive to achieve the highest levels of business integrity through sound corporate governance, internal control and transparency.

Statement of the Problem

Commercial banks in Nigeria including those operating in Enugu State are adversely affected by various forms of corporate frauds because of the recent computerization of bank products and services coupled with the huge financial assets handled by the banks. The recent use of computers, the internet and other electronic devices for banking services in commercial banks in Nigeria has made certain fraudulent activities more efficient, faster and easily concealed. For instance, Ochejele (2004) stated that the incidence of corporate frauds in the Nigerian banking system has become more pronounced in this era of increasing globalization of the financial markets and other economic institutions owing to the use of the internet and the computerization of banking services. Nwude (2006) also stated that the advent of computerization, the use of the internet and other electronic systems in commercial banks in Nigeria have introduced new technology-based frauds which when committed successfully would become difficult to detect. Such frauds, according to him, continue to multiply the financial losses of banks to an unimaginable dimension.

The number of commercial banks in Nigeria since 1892 when the first commercial bank in Nigeria was established has not increased steadily because of intermittent bank failures mainly caused by frauds. The statistics of failed banks in Nigeria show that the licenses of about 50 commercial banks were revoked by the Central Bank of Nigeria between 1994 and 2006. Kalu (2009)

stated that most of the banks went distress as a result of huge financial losses resulting from insider abuse and other fraudulent means including collaboration of bank officials with third parties. Aderinokun (2007) also stated that Nigerian commercial banks lose billions of naira every year and had lost more than N48 billion between 2001 and 2006 to various forms of fraudulent activities.

The prevalence of fraudulent activities in commercial banks has resulted to poor image and low credibility to commercial banks in Nigeria. Consequently, foreign investment inflow into Nigeria is restricted. Corporate frauds greatly devastate the assets and revenues of commercial banks in Nigeria as well as the trust and confidence of the stakeholders of the commercial banks. Udegbunam (2004) stated that corporate frauds heavily undermine the business and profit of commercial banks which most times result in highly risky and volatile financial environments that led to the collapse of many commercial banks in Nigeria.

In order to stay afloat in their commercial activities, commercial banks in Nigeria install and utilize corporate fraud control and prevention systems to fight the scourge of corporate frauds. However, there was doubt whether the corporate fraud control and prevention systems were adequately available, extensively utilized, and effective in the control and prevention of fraudulent activities in the commercial banks. It was also suspected that the commercial banks were encountering some problems in the utilization of the corporate fraud control and prevention systems. An identification of the necessary strategies for enhancing the effective utilization of the corporate fraud control and prevention systems in the commercial banks was, therefore, imperative.

Based on the foregoing, there was the need to determine the corporate fraud control and prevention systems in commercial banks in Enugu State of Nigeria.

The Purpose of the Study

The major purpose of the study was to determine the corporate fraud control and prevention systems in commercial banks in Enugu State. Specifically, the study was to:

1. ascertain the corporate fraud control systems available in commercial banks in Enugu state.
2. ascertain the corporate fraud prevention systems available in commercial banks in Enugu State.
3. find out the extent of utilization of corporate fraud control systems in the commercial banks.
4. find out the extent of utilization of corporate fraud prevention systems in the commercial banks.
5. determine to what extent corporate fraud control systems are effective in the commercial banks.
6. determine to what extent corporate fraud prevention systems are effective in the commercial banks.
7. identify the problems encountered by the commercial banks in the utilization of the corporate fraud control and prevention systems.
8. explore the strategies for enhancing the effective utilization of the corporate fraud control and prevention systems in the commercial banks.

Significance of the Study

The findings of this study would be beneficial to the management of commercial banks, bank customers, investors and the Ministry of Commerce

and Industry in Enugu State. The result of this study would also be of immense benefit to the teachers and students of Business Education in tertiary institutions in Nigeria. Firstly, the findings of this study would assist the management of commercial banks to establish stronger defences against fraudulent activities. The frequency of fraud occurrence in the banks as well as losses would be drastically reduced by enhancing the utilization and effectiveness of the corporate fraud control and prevention systems in the banks. The findings of this study would also enable commercial bank managers to evolve more sustainable risk management policies against fraudulent activities. The accountants would be able to control corporate risks effectively with improved capacity in fraud risk management. The findings of this study would assist the commercial bank managers to improve their capacity building initiatives for banking services especially for fraud control and prevention. The result of this study would also enable the credit and loan managers of commercial banks to achieve their financial targets and corporate governance goals through extensive and effective utilization of the fraud control and prevention systems in the banks.

The awareness of the availability, the extent of utilization and the effectiveness of the corporate fraud control and prevention systems in the commercial banks would enhance the customers' trust and confidence in the commercial banks. The customers' patronage of bank products and services would also increase. Fresh customers would also join the present customers of the commercial banks to patronize the banks' products and services. The general business and profit of the commercial banks would, therefore, increase through improved customer patronage of bank services.

Investors in Enugu state would also benefit from the findings of this study. An understanding of commercial banks' capacity in fraud control and prevention would assist the investors in their investment decisions. The present investors of commercial banks would be encouraged to maintain their investments in the banks while prospective investors would be stimulated to make fresh investments in the banks. The outcome of this study would also help to improve the commercial banks' returns on investments to the investors.

The Ministry of Commerce and Industry in Enugu state would also gain from the findings of this study, especially as it concerns the effectiveness and utilization of the fraud control and prevention systems in commercial banks in Enugu State. The findings of this study would assist the ministry in its campaign for efficient banking services and operations in the state. The findings of this study would assist the Ministry of Commerce and Industry on making policies that would encourage effective participation of the commercial banks in economic development of the state. Better corporate governance practices that would arise from the findings of this study would increase the commercial banks economic, environmental and social responsibilities in Enugu state.

The outcome of this study would significantly be of immense benefit to both the teachers and students of Business Education in tertiary institutions in Nigeria. The result of this study would assist them in the teaching and learning of the subject. Curriculum experts in Business Education would use the facts of the findings in curriculum planning and review. The graduates of Business Education would be guided by the outcome of this study in the teaching and practice of fraud control and prevention in their different places of work

especially as it affects the availability, the extent of utilization and the effectiveness of the corporate fraud control and prevention systems in commercial banks and other corporate organisations in Nigeria.

Finally, the results of the study would be a significant addition to the literature base of corporate fraud control and prevention systems in commercial banks in Nigeria. The findings of the study would provide much empirical evidence on the adequacy, extent of utilization and effectiveness of corporate fraud control and prevention systems in the commercial banks. The findings of this study would also provide a better understanding of the theoretical basis of the corporate fraud control and prevention systems utilized in commercial banks and other corporate organisations.

Research Questions

The following research questions were answered for this study:

1. What are the corporate fraud control systems available in commercial banks in Enugu state?
2. What are the corporate fraud prevention systems available in commercial banks in Enugu state?
3. To what extent are the corporate fraud control systems utilized in the commercial banks?
4. To what extent are the corporate fraud prevention systems utilized in the commercial banks?
5. How effective are the corporate fraud control systems in controlling frauds in the commercial banks?
6. How effective are the corporate fraud prevention systems in preventing frauds in the commercial banks?

7. What are the problems encountered by the commercial banks in the utilization of the corporate fraud control and prevention systems?
8. What are the strategies for enhancing the effective utilization of the corporate fraud control and prevention systems in the commercial banks?

Hypotheses

The following hypotheses formulated for this study were tested at 0.05 level of significance:

Ho_1: There is no significant difference in the mean responses of management staff in new and old generation banks on the extent of utilization of the corporate fraud control systems in the commercial banks.

Ho_2: There is no significant difference in the mean responses of management staff in new and old generation banks on the extent of utilization of the corporate fraud prevention systems in the commercial banks.

Ho_3: There is no significant difference in the mean responses of management staff in new and old generation banks on the effectiveness of the corporate fraud control systems in controlling frauds in the commercial banks.

Ho_4: There is no significant difference in the mean responses of management staff in new and old generation banks on the effectiveness of the corporate fraud prevention systems in preventing frauds in the commercial banks.

Ho_5: There is no significant difference in the mean responses of management staff in new and old generation banks on the

problems encountered by the commercial banks in the utilization of the corporate fraud control and prevention systems.

Delimitation of the Study

This study was delimited to the corporate fraud control and prevention systems in commercial banks in Enugu state. No attempt was made to investigate the corporate fraud control and prevention systems in commercial banks in other states of the federation of Nigeria.

CHAPTER TWO
REVIEW OF RELATED LITERATURE

The review of the related literature for this study is presented under the following headings:

Conceptual Framework

- An overview of the general concepts of corporate fraud control and prevention systems in commercial banks
- Corporate fraud control systems available in commercial banks
- Corporate fraud prevention systems available in commercial banks
- Utilization of corporate fraud control and prevention systems in commercial banks.
- Effects of corporate fraud control and prevention systems in commercial Banks
- Problems encountered by commercial banks in the utilization of corporate fraud control and prevention systems
- Strategies for enhancing the effective utilization of corporate fraud control and prevention systems in Commercial Banks

Theoretical framework

Related empirical Studies

Summary of the Related Literature

Conceptual Framework

- **An overview of the general concepts of corporate fraud control and prevention systems in commercial banks**

The first commercial bank in Nigeria was established in 1892. The bank was the African Banking Corporation established by the British West Africa.

The bank is now called First Bank of Nigeria Plc. The number of commercial banks in Nigeria has since then increased (Aigbokhaevbolo, 2001). Prior to the conclusion of the banking industry consolidation exercise in December 2005, 89 commercial banks operated in Nigeria. However, 25 commercial banks survived the consolidation exercise and are currently operating in their branches all over the country (CBN, 2006). Meanwhile, the number has reduced to 24 after the merger of Stanbic and IBTC banks in 2007. Aderinokun (2007) sated that there were 3866 commercial bank branches in Nigeria up from 3200 prior to the conclusion of the consolidation exercise. The consolidation exercise increased the capital base of each bank to a minimum of N25 billion.

Commercial banks are financial institutions which accept fund deposits for the purposes of safekeeping, lending and investment as well as allowing the withdrawal of the fund on demand by the depositors (Nwude, 2006). Commercial banks are those corporate financial institutions that accept financial deposits that can be withdrawn on demand by the depositors. The commercial banks provide the institutional framework for the implementation of monetary policy and its transmission mechanism (Anyanwokoro, 1998).

The above definitions of commercial banks recognize commercial banks as institutions that accept financial deposits that can be withdrawn on demand by the depositors. However, Nwude's definition differs from Anyanwokoro's because he included the safekeeping, lending and investment of the deposited funds in addition to withdrawals made by depositors. Anyanwokoro also differed from Nwude in his own definition by stating that commercial banks are corporate financial institutions that provide the institutional framework for

the implementation of monetary policies and the transmission mechanisms. The definitions have some similarities with few differences. None of the definitions included that commercial banks perform those functions because of their charter which gives them the authority. For the purpose of this study, commercial banks are regarded as corporate financial institutions that accept monetary deposits from customers, effect withdrawals on demand, grant loans and provide other services to customers as authorized by their charter.

Sanusi (2003) stated that commercial banks perform the crucial role of financial intermediation, thus influencing savings and investments as well as facilitating the effectiveness of monetary policy. Commercial banks are the major provider of liquidity to the economy. They are the principal depositories of the public financial savings and the managers of the nation's payment systems and fund transfers.

The importance of commercial banks in Nigerian economy derives from their roles in financial intermediation, provision of an efficient system of payment and fund transfers. They also facilitate the implementation of the monetary policies initiated by the Central Bank of Nigeria (Nduka, 2001). The financial intermediation of commercial banks, according to Nduka, involves the mobilization of savings from the surplus units of the economy and channelling the funds by way of lending and investments to the deficit units to expand the productive capacity of the economy.

Nduka (2001) further stated that the commercial banks while performing the intermediate functions ensure the protection of depositors, encourage healthy competition and maintain the banks' stakeholders' confidence in the stability of the banking system. Obi (2002) listed the services provided by

commercial banks to include monetary transfers, provision of bank loans and credit cards, stock broking and foreign exchange services. The Nigerian Commercial Banks are also presently providing Automated Teller Machine (ATM), Electronic Point-of-sale (POS) Terminal, Internet Banking (I-baking) and mobile banking services which are SMS-Based.

Commercial banks in Nigeria are currently operating on full-time electronic platform. The introduction of on-line and electronic real-time banking services in Nigeria together with the increased capitalization of the banks has resulted in new payment systems and funds transfers amidst heavy competition among the banks (Ogbulie, 2007). The new payment systems and fund transfers organized electronically and online together with the huge financial assets handled by Nigerian commercial banks have made the banks highly vulnerable to corporate frauds.

Fraud is a category of crime that involves an individual or a group of individuals dishonestly obtaining property or some financial advantage by means of deception (Smith, 1999). The perpetrators may seek to gain money, property or information about opportunities to commit fraudulent activities. Zervos (1999) stated that fraud is an art of deception for gain, and dishonesty is an essential ingredient. He stated that fraud varies in type, size and complexity. He further stated that frauds are encountered in different contexts and they change as the society changes with all its different attitudes and technological advancement. Smith (1999) stated that the offenders of fraudulent activities might be customers, employees or managers of corporate organizations in both the public and private sectors of an economy.

Frauds can occur to individuals and also to business organizations. Fraudulent activities occurring in a business environment are called corporate frauds. Corporate frauds involve misappropriation, theft or embezzlement of corporate assets in a particular business environment (Jenfa, 2002). Corporate frauds, whether within or outside a business environment, are caused by the will to commit fraud, the opportunity to execute the fraud and the exit which is the escape from sanctions against successful or attempted fraud. Jenfa summarized the three elements as the Will, the Opportunity and the Exit (WOE) of fraud.

According to Levy (1999), corporate fraud involves deception, misappropriation, and misrepresentation of a company's assets or the manipulation of its financial data to the advantage of the perpetrator. Corporate frauds affect businesses, large or small, especially financial institutions, which include commercial banks (Shackell, 2000). According to Shackell, new technologies such as the Internet, computers and the development of fully automated accounting systems with various electronic on-line products for banking have increased the opportunities for fraudulent activities in commercial banks. Usman (2004) agreed and stated that the computerization of banking services and the introduction of electronic and on-line products in banking have significantly escalated the incidence of fraudulent activities in commercial banks.

According to Nwude (2006), corporate fraud is the number one threat to business and it is becoming predominant in banking industry. Nwankwo (1999) also stated that nowhere is fraud more serious than in banking as it is the biggest cause of bank failure. He also stated that the magnitude of the problem

of fraudulent activities and its implications have been an enormous task to commercial banks.

Nwude (2006) defined bank fraud as the act of misappropriation of bank assets either in cash or in kind by bank staff, bank customers or third parties in which the bank suffers losses arising from such acts. He stated that bank fraud is a wicked act that confers illegal possession of other people's wealth on the fraudulent person thereby preventing the original owner(s) from enjoying the wealth. Nwude further stated that the intention of the fraudulent person in bank fraud is to dishonestly benefit himself to the detriment of the bank, bank staff, bank customers or any other member of the public through banking activities.

Bank frauds can be committed by bank staff, customers and third parties (that is non-banking customers) and a combination of the bank staff, customers and third parties. The fact that commercial banks deal in money and instruments that can easily be converted to cash, and the ultimate ambition of the fraudulent persons is to get rich quickly the commercial banks have become persistent targets for fraudulent activities (Nwude, 2006). Nwude stated that the advent of computerization in commercial banks introduced new technology-based frauds which when committed successfully would become difficult to detect. Such frauds continue to multiply the financial losses of banks to an unimaginable dimension.

Corporate frauds, especially in banks, devastate the assets and reputation of a business organization, the trust and confidence of its customers (Quova 2005). Smith (1999) lamented that corporate frauds affect all stakeholders of an organization including the general public and is of particular concern to those who manage large corporate business organizations where the potential losses

are greatest. According to Zervos (1999), fraud is generally covert and very difficult to detect. He stated that the perpetrators employ a lot of ingenuity and sophistication to conceal the way in which the fraud is committed.

The increase in account frauds and 'phishing' in financial institutions has made it critical for every commercial bank to install and implement modern corporate fraud control and prevention systems (Quova, 2005). 'Phishing' is the technique of using falsified e-mails and bogus websites to dupe users of bank products. This is done by causing the users of those products to surrender their personal data that can be used to steal their identities and access their bank accounts. Sanusi (2003) stressed on the need for commercial bank authorities to establish necessary fraud control and prevention systems to fight the scourge of corporate frauds. He advised that adequate fraud control and prevention should be the paramount of commercial banks because fraud undermines the public confidence in the system and can force sudden contraction of money supply in the economy. He also stated that the scourge of corporate frauds in commercial banks can subsequently cause failure of the payment system.

The American Institute of Certified Public Accountants, AICPA (2002) stated that the risk of corporate fraud could be reduced through a combination of control and prevention measures. The institute also stated that frauds could be difficult to detect because it often involves concealment through falsification of documents and collusion among management, employees and third parties. It is, therefore, important to place a strong emphasis on fraud control, which could persuade fraudulent persons not to commit fraud because of the likelihood of detection and punishment. Emphasis should also be on fraud prevention, which reduces the opportunities for fraud to take place. More so,

fraud control and prevention measures are much less costly than time and expenses required for fraud detection and investigation.

According to Shackell (2000), the challenge for organizations including commercial banks is to develop corporate fraud control and prevention systems, which will thwart even the most determined and skilled professional fraudster, while at the same time discouraging the opportunist from making any attempt to commit fraud. He also stated that the management of businesses should sometimes consider conducting an evaluation of the fraud control and prevention systems that are available. Such evaluation, according to him, should consider the availability of the systems, the level of implementation and the effectiveness of the systems.

A system is defined by Osuala (1998) as a group of interdependent items regularly interacting to form a unified whole. According to Ile (1999), a system is a set of interdependent parts that perform different related functions to achieve the objective of the whole. He stated that it involves a series of procedures, methods and controls designed to operate together in order to achieve a pre-planned objective. The parts that make up the system are the subsystems, which must function interdependently to achieve the objective of the system. The corporate fraud control and prevention systems are the different methods and procedures set by the management of a business to reduce the incidence of fraudulent activities and their effects to the business organization.

The strategies adopted by business organizations to control and prevent fraudulent activities are many. They range from the most general policy statement designed to ensure the efficient conduct of business to the highly

specific information and systems offered to enable people avoid the temptation of committing fraudulent activities to the organization (Smith, 1999). Corporate fraud prevention, according to Smith, involves complex and sensitive processes of balancing an organization's diverse interests to safeguard the limited resources. According to Achaka (2004), fraud prevention seeks to establish series of physical, logical and procedural barriers to discourage fraudulent incidents. It involves the implementation of cost-effective counter measures to reduce the impact of fraud scourge identified by risk management in an organization.

According to Shackell (2000), there is no foolproof method of preventing fraud but there are techniques that have proven successful. He stated that the techniques might be used to test for fraud profile and to prevent fraudulent occurrence. He further stated that corporate frauds may not be totally eliminated but they can be controlled.

Osasebor (2004) described corporate fraud control systems as moral checks put in place by the management of a corporate business organization to make fraud more difficult to commit. The fraud control measures, according to him, are also to make the chance of detecting fraud much easier where it has been committed. He also stated that the opportunity to commit fraudulent activity motivates the perpetrators to commit fraud. Fraud opportunity reduction should, therefore, be the fundamental principle of an effective fraud control system since both motivation and opportunity must come together in order for fraud to be committed. The relationship of motivation and opportunity must always be considered when structuring an effective fraud control and prevention system.

Effectiveness is the achievement of the set objectives. It refers to the extent to which output is in line with organizational objectives (Ile, 1999). Goetz (1968) in Ile (1999) defined effectiveness as the degree to which the resulting output and performance satisfies the predetermined objectives. A system is said to be effective if it does the right thing it was designed to do (Drucker, 1974 in Eze, 2006). Onah (2003) defined effectiveness as the degree of success expected which is obtained from a method or procedure.

An effective fraud control and prevention system can reduce fraudulent activities with minimum expense, waste and effort. The system should be cost-effective to the organization that established it (Smith, 1999). Smith also stated that some corporate fraud control and prevention systems may be effective in terms of reducing fraudulent means but may have the consequences of stifling commerce and making everyday business transactions so unwieldy and costly to manage. He further stated that fraud control and prevention systems should, therefore, aim at maximizing crime reduction without imposing unrealistic burden on legitimate business activities.

According to the American Institute of Certified Public Accountants, AICPA (2002), some organizations significantly have lower levels of misappropriation of assets and are less susceptible to fraudulent financial activities than other organizations. It is because they take proactive steps to control and prevent frauds. The Institute stated that it is only those organizations that seriously consider fraud risks and take proactive steps to create the kind of climate to reduce the incidence of fraud that have success. The management of an organization is responsible for designing and implementing the systems for the control and prevention of frauds. This is done

to ensure a culture that promotes honesty and ethical behaviour while striving to achieve the overall organizational objectives.

- **Corporate Fraud Control Systems Available in Commercial Banks**

Fraudulent activities in commercial banks can be reduced through robust fraud control systems. Onyekwelu (1998) stated that the corporate fraud control systems in commercial banks are the various strategies applied by banks for fraud avoidance and fraud minimization. She stated that bank frauds may not be totally eliminated but they can be minimized by using appropriate fraud control measures. She further stated that the nature of frauds determines the type of control measures adopted by an organization. For instance, she stated that for credit fraud risks, adequate credit evaluation, supervision, credit monitoring and appraisal are required.

According to Sanusi (2007), for commercial banks and other financial institutions to effectively reduce the incidence of fraud, they should focus on the following fraud control measures: paying equal attention to both the quantifiable and unquantifiable fraud risks, identify and report possible fraudulent opportunities and let an awareness of fraudulent opportunities and their consequences pervade the entire organization. He stated that commercial banks should make fraud control everybody's responsibility. He further stated that fraud control measures deliver values and that they should be enshrined in commercial banks' corporate culture.

Aderibigbe (1999) stated that modern commercial banks establish fraud control and operating procedure that match with computerization and on-line banking. He also stated that commercial banks should have written operating procedure manual as well as functional internal audit department to promote

the effectiveness of the fraud control and prevention systems. He further stated that a qualified accountant should head the internal audit department to ensure the effectiveness of the section in fraud control and prevention.

Fraud control systems are moral checks put in place in commercial banks to ensure reduction of fraudulent opportunities (Osasebor, 2004). Osasebor stated that an employee with fraudulent intention who knows that he is under surveillance would be deterred from making an attempt to commit fraud. He stated that the way to remove fraudulent opportunities is to institute some measures of best practices in fraud control. Some of the measures, according to him, are fraud awareness and education, personnel and transaction monitoring, improvement in personal identification and counterfeit prevention.

According to Jenfa (2002), fraud control in commercial banks starts with the control of people. The people are the bank employees, bank customers and the general public who visit the banks. Commercial banks can organize the staff by effectively installing suitable organigram that is easy to understand. Jenfa stated that appropriate authority at each level should be provided to evolve a more result-oriented and accountable management based on performance and integrity. He also stated that talented goal-oriented staff and management whose future is linked with the fortunes of the bank should be engaged in the implementation of the fraud control systems.

Jenfa (2002) further stated that the discipline of staff of commercial banks is very important to ensure at least the minimum level of conformity, orderliness and accountability below which the bank will not be able to perform. The control measure here ensures that people with the appropriate level of education and training are engaged across board. There must be an

adequate need-related incentive and motivation of the bank employees. The employees must be exposed to on-the-job training and retraining programmes.

According to Ochejele (2004) corporate fraud control in commercial banks should involve the selection of employees of the right characteristics and education. There should be appropriate remuneration and promotions as well as career development prospects for the employees. He stated that all commercial bank operations should be supervised adequately. The responsibility for the supervision, according to him, should be clearly defined and communicated to the person(s) being supervised.

Smith (1999) stated that one of the most effective strategies adopted for fraud control in modern commercial banks is the education of the staff and customers. He stated that this is based on the nature of the fraud risks they face and how those risks can be avoided. He stated that fraud awareness and education should be made available to the entire employees in a banking environment. Smith further stated that commercial banks should involve high profile publicity and education campaign for payments of cheques and clearing services through the use of posters, leaflets, and television and radio coverage. He stated that this is done to raise the public awareness on the problems of bank frauds and to encourage the bank customers to take stringent care of their transactions and their banking instruments.

Smith (1999) further stated that modern corporate fraud control programme in commercial banks also include established fraud policies, pre-employment integrity screening and monitoring of staff. He stated that there exists software for analyzing bank transactions as well as payment authorization. He also stated that centralized fraud reporting is also used to

reduce card payment and transaction frauds in commercial banks. Computers used in commercial banks contain programmes designed to assist in controlling various fraudulent activities in commercial banks. Vittal (1999) stated that those programmes could be highly vulnerable because personnel with powerful privileges can manipulate access to computer terminals or files. He stated that it is imperative that commercial banks are aware of the vulnerable points in the computer systems to guard against fraudulent behaviours.

The American Institute of Certified Public Accountants, AICPA (2002) identified many corporate fraud control measures that are used in commercial banks. They include the creation and maintenance of culture of honesty and high ethics, the evaluation of fraud risks and the implementation of the processes, procedures and controls needed to reduce the opportunities of fraudulent activities. The Institute also stated that commercial banks also undertake oversight processes. They also provide incentives and motivation to their staff by creating positive workplace environments. The bank employees are also motivated through regular promotion and training (AICPA, 2002). According to AICPA, the anti-fraud processes of commercial banks as well include identification and measurement of fraud risks and mitigation of fraud risks. The implementation and monitoring of an appropriate internal control system is also one of the processes of fraud control adopted by commercial banks.

According to Shackell (2000), the identification of the high fraud risk areas in the transactions of commercial banks is the first step in corporate fraud control. He stated that a typical fraud analysis will involve physical inspection of important sections, detailed examination of company's policies and

procedures, interviews with key employees, examination of account records, computer systems and corporate documents. He stated that commercial banks' corporate fraud control system should state in clear terms the corporate and security policies of the banks. The corporate policy document should set out the fraud control guidelines and the consequences of fraudulent action or withholding of information concerning any such action. The comprehensive policy document should be prepared by the bank management and made available to all employees. He further stated that the employees should be required to sign a declaration that they have read and understood the policy requirements. According Shackell (2000), a commercial bank's corporate and security policies should spell out the bank's stand on acceptance of gift and entertainment, conflict of interest, criminal and civil redress against an erring employee.

Shackell (2000) further sated that commercial banks' corporate fraud control strategies incorporates staff pre-employment screening as part of the banks' standards for recruitment. The aim is to avoid employing criminals and candidates with false qualifications unwittingly in high security or sensitive positions. He stated that the pre-employment screening should involve interviews with the referees and past employers of the candidates. The exercise, according to Shackell, should also involve independent verification of educational certificates and relevant background searches through an on-line database.

Nduka (2001) recommended that modern commercial banks' corporate fraud control systems should include authorization of transactions procedure, segregation of duties and adequate electronic recording of transactions. He also

recommended the use of closed-circuit technology to record and monitor the movement of bank staff, customers and other third parties in the banking environments. He stated that this system may have negative effect on staff but explanation should be given to them on the importance of the device. Nduka, further stated that the establishment of internal audit and disciplinary committee unit in commercial banks should be an essential part of commercial bank's fraud control systems. Smith (1999) also identified effective internal control, supervision of personnel, and analysis of transaction patterns as key elements of an effective fraud control programme.

Nwude (2006) identified the following fraud control measures in commercial banks: enactment of anti-fraud rules and regulations, recruitment policies and reward systems of bank staff. He also stated that the fraud control measures include the posting, placement, job rotation and disengagement procedures of staff. He further stated that regular training and retraining of staff are prerequisites of a corporate fraud control system. According to Zervos (1999), if the staff and customers of commercial banks are comprehensively educated about the existing fraud opportunities and the consequences of utilizing the opportunities, they will understand their obligation and responsibilities on how to fight the problem of fraudulent activities. He further stated that the awareness derived from fraud education could stimulate the bank employees and customers for integrity building.

- **Corporate Fraud Prevention Systems Available in Commercial Banks**

Corporate fraud prevention systems are series of physical, logical and procedural barriers established to discourage fraudulent activities. It aims at

implementing cost-effective counter measures that can prevent or reduce the impact of fraud threats identified by risk assessment (Achaka, 2004). At the heart of any corporate fraud prevention system is the effective, efficient and secure management of information. He stated that information is a key asset and is the product of people interacting with processing systems, technology and raw data. He further stated that the management of information involves the maintenance of confidentiality, integrity, availability and accountability of the information. Robust physical, environment and corporate security controls are integral parts of the information management. Achaka also stated that information management is a primary measure in corporate fraud prevention and a key element in establishing acceptable standards of corporate care in an organization.

Smith (1999) stated that commercial banks are now using neural networks in the prevention of electronic fund transfer frauds. He also stated that there are software devised to analyse plastic cardholder spending patterns in order to alert customers on the presence of unauthorized transactions. There are software created to maintain records of lost cards, stolen cards and counterfeit cards.

Nestor (1998) stated that payment authorization is one of the main strategies used by commercial banks to prevent debit and credit card frauds. He stated that this system lowers the floor limits, which is the transaction value at which authorization is required from the commercial banks or bank branches before the card can be accepted. This strategy along with the introduction of "Hot Card File" or database of stolen cards, according to him, has led to drastic reduction in Electronic Point-of-sale (EPOS) fraud. Another strategy that has

been highly successful, as stated also by Nestor (1998), is the positive pay system by various banks. Commercial banks and other financial institutions through this system are provided by business organizations electronic lists of cheques issued each day, which are immediately reconciled by banks with the cheques actually presented. Any forged or altered cheques are detected and payment stopped.

Smith (2000) stated that commercial banks are now offering real-time payment authorization for transactions above the specific floor limits. He further stated that commercial banks generally encrypt electronic data in order to secure electronic fund transfers using algorithm that encode messages. The messages are then decoded using electronic key known to both the sender and the receiver. Meijbourn (1998), however, stated that the major security risk associated with the encryption system is the possibility of encryption keys being revealed or manipulated. He stated that most of the large-scale electronic fund transfer frauds, which have been committed in the past, have involved interception and alteration of electronic data messages transmitted from computerized financial institutions. However, he stated that commercial banks are now using payment protocol called 'SET' (Secured Electronic Transaction) developed by Microsoft and VISA. This system uses public key encryption to protect data from being compromised. Digital signatures and screening software are also used to authenticate the parties involved in the fund transfer as well as the information intermediaries on loans and mortgages offered on-line.

According to Johnson (1999), the most successful corporate fraud prevention measures used by commercial banks to prevent false identity frauds

based upon altered and/or counterfeit documents involves improving the reliability of evidence used for personal identification. He stated that biometric identification systems which make use of an individual's unique physical characteristics like finger prints, voice patterns, retinal images, facial and hand geometry, subcutaneous vein structure and body odour are used by commercial banks. Database of customers and their characteristics are maintained by the banks for this purpose.

Smith (2000) stated that a wide range of security features for plastic cards, cheques and banknotes have been developed and are used in commercial banks to combat counterfeiting frauds. He also stated that standard cheque security features include laid lines, colour prismatic printings, void pantographs, warning bands, holograms, etc. He further stated that cards are protected by security printings, micro spring holograms, tamper evident signature panels, magnetic stripes with improved card validation technologies and indent printing. The card validation technologies, according to Smith, are personal Identification Number (PIN) and passwords.

Bank frauds in recent times have been facilitated through the use of computers. Fraud prevention initiatives, particularly in electronic and on-line banking, have sought to protect computers and computer networks from interference and manipulation (Smith, 2000). With the ever-developing sophistication of computer systems, according to Smith, continued effort is directed at preventing computer frauds through effective management and monitoring of information technology systems. For instance, ATM and ETPOS terminals are located in secure places where users are protected physically from

shoulder surfing to obtain PINs and passwords. ATMs are even placed in lobbies with card access under security guards.

According to Quova (2005), one tool that has become a standard for fraud prevention in commercial banks is the web geography technology known as geolocation. Geolocation is the system of determining the true geographical location of the on-line customer. Quova stated that geography is a proven fraud indicator and geolocation has established itself as a critical underpinning technology that enables the on-line commercial banks to do business with confidence. Geolocation technology identifies the geographical location of any on-line visitor to an e-banking website in real time from the country of origin down to the city level with precision. Quova (2005) further stated that geolocation employs a combination of technologies, data gathering systems and human expertise to identify the users' location. Geographical information can provide clues to possible frauds. For example, out-of-state cheques call for additional scrutiny. This will enable the commercial bank to compare the user's true location with the address on the account or application.

Reynolds (2006) identified facial recognition technology as one of the fraud prevention systems adopted by commercial banks to solve personal identification and authentication fraud problems. He stated that identity fraud is a simplistic crime where anybody could become known easily. He further stated that facial recognition technology is one of the biometric identifiers that has wide public acceptance and is considered the least intrusive of all other technologies. He also stated that enrolment could be passive because a person entering the bank hall that is equipped with facial recognition technology is automatically enrolled into the system. There are many biometric identifiers

but specific application of facial recognition to reduce fraud by targeting cheque fraudsters involves one-on-one over-the-counter transaction. Facial recognition, according to Reynolds, has the potential of preventing fraud in over-the-counter transaction. He stated that what is needed is earlier detection of the fraudster by giving the bank staff time to react and respond to the fraudster before he/she can complete the criminal transaction.

According to Abagnale (2005), technology breeds crime but the new technologies such as facial recognition is capable to deter and prevent bank frauds. He stated that there are several biometric technologies that use pattern recognition to verify an individual's claimed identity. He further stated that biometric identifiers like facial recognition are used to validate an individual who conducts financial transactions in the bank.

Linniit (2006) stated that commercial banks make checklists of suggestions on the prevention of corporate frauds available to their customers. He also stated that this checklists are made available to the customers inform of leaflets, posters and pamphlets. Some banks also give such information through the radio, Television and newspaper. The information usually found in the checklist, according to him, include the following: keep your cards in sight when making transactions to avoid fraudsters counterfeiting or stealing the cards, look after your card, keeping it secure at all times and don't let off your sight from the card when making transactions and carefully discard your bank statements by shredding them to prevent "bindivers" from acquiring information about you and your account. Other items that can be found in the list are: always check your bank statement and contact your card issuing bank immediately if you find any unfamiliar transaction therein and never write

down your Personal Identification Number (PIN) and never disclose it to anyone. Linnitt (2006) also stated that the checklist also contains such statements as: report lost or stolen cards to your card issuer immediately and be wary of anyone who might be trying to watch you enter your PIN and do not allow yourself to be distracted by any one trying to talk to you. He finally stated that in any country, the security of plastic cards and the information therein is reliant on the issuing banks own protocols, systems and security levels.

Charlton and Taylor (2004) identified electronic authorization as the most basic technique utilized by commercial banks for corporate fraud prevention in the banking environment. This process verifies that the money-withdrawing instrument like plastic cards and cheques are valid and has sufficient fund attached to it in the account. They stated that for plastic card transaction, a system involving microchips and personal Identification Numbers (PIN) are currently used. Microchips are added to the cards to store data securely and PIN is used rather than signature at the point of withdrawal. The chip and PIN cards use chip readers and PIN pads attached to the computer to provide more secure transaction technology. Charlton and Taylor further stated that other additional on-line fraud prevention systems utilized by commercial banks are Address Verification service (AVS), Card Verification Number (CVN), Positive Pay (V-pay) and Verified by Visa (VBV). They stated that encryption of data is also a prevention strategy used by commercial banks.

According to Charlton and Taylor (2004) commercial banks usually use the payer authentication option offered by the card issuing companies like

Mastercard and VISA International. The payer authentication option makes use of password. Payments are only authorized if the customer knows the password since this makes it more likely that the person making the withdrawal is in fact the genuine cardholder. Commercial banks also keep database of both the good and bad customers to be at alert.

According to Osasebor (2004), corporate fraud prevention in commercial banks involves more than risk assessment, monitoring and supervisory review. He stated that commercial banks develop specific instruments to deal with specific kinds of frauds. For instance, he stated that bank transactions on the Internet or any digital equipment no longer involve signatures. This is because anybody can cut out the signature and paste it on something else and then use it to advantage. That is for some ulterior motives. He further stated that passwords and personal Identification Numbers (PINs) are used in Internet and plastic card banking transactions instead of signatures.

Commercial banks create appropriate firewall technologies and password software to strengthen the banks defences against electronic and on-line fraudulent activities (Usman, 2004). He stated that commercial banks establish overt surveillance systems that are easily visible to the public and staff in the banks. These systems prevent certain frauds from occurring as the potential fraudsters are deterred from committing the act of fraud due to swift detection characteristic of the system.

Smith (1999) stated that the most frequently used strategy for the perpetration of bank frauds is the creation of false identity based upon altered and counterfeit documentation. He also stated that the most successful counter measure is the improved reliability evidence used for personal identification

since authenticating one's identity is very crucial in preventing computer-based frauds. He further stated that some security measures adopted by commercial banks in this regard are password security, challenge–response protocols and call-back systems. These methods, according to him, have been devised by commercial banks to authenticate the identity of the real customer(s) of the bank. Smith (1999) also stated that commercial banks adopt geodetic methods to ascertain the location of the customer at the point of an on-line and electronic transaction in real- time. The geodetic method make use of location signature which utilized signals transmitted by satellite in order to determine a location on earth of any user who attempts to gain access to the banking systems.

Commercial banks, according to Shackell (2000), have developed computer forensic systems in response to trends in corporate fraudulent activities. Shackell stated that computer forensic is the seizure and analysis of electronic data using a methodology that ensures future admissibility as evidence of the data in a court of law. He stated that computer forensic have become an integral part of electronic corporate fraud prevention. He further stated that the fundamental principle of computer forensics is that the original data is never altered. He stated that written image software is used to capture an exact copy of target computer system. From this image, according to him, the original system can be recreated at any point in time. This method ensures the integrity of the target system.

The existence of computerized systems and the upgradation of the systems in commercial banks have helped immensely in bank fraud prevention

(Vittal, 1999). Vittal stated that commercial banks use signatures captured in the computers, stop-payment instructions stored in the computer and prompt reconciliation of amount and number of cheques through computerized systems to prevent frauds in banks. Magnetic Ink Character Recognition (MICR) and electronic clearing systems of cheques as well as computerized databases of parties enjoying credit facilities from different banks in the same centre are used to avoid double financing under different names. He further stated that database of information on fraudsters are also maintained. There is also quick exchange of information in relation to transactions in corporate accounts. These are maintained through inter and intra bank connectivity.

According to the Bank of Netherlands (2006) fraud preventive measures are designed by banks to ensure that events, which threaten operations in banks, do not occur or occur infrequently. The banks stated that some of the preventive measures adopted by commercial banks against fraudulent activities are careful designing and locating of computer centres, security devices to prevent unauthorized access to computers and password designed to restrict access to data in the computer. Others are the authentication of telecommunication messages and the testing of computer and other systems before their implementation. The fraud preventive measures, according to the bank, are essential for the effectiveness, integrity and reliability of bank operations.

Clark (1998) stated that one of the modern fraud prevention systems used in commercial banks is dataveillance. He defined dataveillance as a system of monitoring people's actions and communications through the

application of information technology. He stated that the system could be used to monitor one or a group of persons. According to him, dataveillance integrates data hitherto stored in various locations of commercial bank branches to screen and authenticate people and transactions against internal norms. He stated that the systems could also perform front-end verification of transactions that appear exceptional against data relevant to the matter at hand. The data used could be sought from internal database or external database from other organizations.

- **Utilization of Corporate Fraud Control and Prevention Systems in Commercial Banks**

Commercial banks in Nigeria have in place manuals of operations and ensure due process to protect the integrity of the operations (Ataman, 2007). He stated that commercial banks could be said to be one of the foremost institutions in the country that its operations are computerized. He also stated that commercial banks' staff are mostly educated, well trained and they are dedicated to duty. However, he advised that the staff and management of commercial banks must be careful and focused in the course of their work as errors committed in the banking environment usually have effects of monumental proportions.

Ataman (2007) stated that very common these days in commercial banks are cases of people doing certain things without reflection and thereby creating problems for the innocent person. He stated that staff of commercial banks should be watchful and sensitive because each bank has an anti-corruption unit, which is a vital office. The unit, according to him, records and investigates complaints of corruption and abuse of offices against staff and other

stakeholders. He stated that necessary disciplinary measures are taken against the offenders. He further stated that this is in conformity with the directives of government as part of the measures to deal effectively with corruption in all terms.

According to Okauru (2007), the fight against financial crimes is not an optional action given the grave implications of these crimes on the banking sector. He stated that the fight against financial crimes is vital to the stability of both the domestic and international financial system of the economy. He also stated that it is a fight that calls for unwavering commitment and constant reassessment of the threats and counter measures in order to stay at least one step ahead of the criminals. He further stated that the players in the Nigeria financial system must be creative as well as make concerted effort to put in place and use appropriate measures to close all loopholes which financial criminals can take advantage of because of the dynamism of the criminals. According to him, operators of commercial banks must engage in partnership or strategic alliances with the regulatory and law enforcement agencies for effective fraud control and prevention. Okauru stated that commercial banks should specifically strengthen the financial control polices and operations, look out for fraudulent individuals, make use of "know Your Customer (KYC)" procedures and develop the prevailing anti-fraud solution in the market.

According to Bhaskar (2006), commercial banks review on regular basis their operation including reports on defaulters and take appropriate measures to improve their services. He stated that the banks put up detailed quarterly analysis of all bank operations related complaints to their top management. For

instance, he stated that card-issuing banks have in place suitable monitoring mechanism to randomly check the genuineness of merchant card transactions. He further stated that commercial banks set up control and prevention systems to combat fraudulent activities and actively participate in fraud prevention committee. The fraud prevention committee, according to him, formulate rules to prevent frauds and take proactive fraud control and enforcement measures.

Ugwunna (1998) stated that most commercial banks are found to have employed adequate number of fraud control and prevention systems. He stated that because there exist some misconceptions of the measures by both the customers and banks staff, staff sometimes violate and render the systems ineffective through ignorant collaborations. However, Avey (2004) stated that it is vital to recognize that there are limits to technological and procedural controls and preventive measures against corporate frauds. He also stated that given the speed with which computer and data communication technology evolve and the complexity of modern systems it is difficult for improvements in fraud prevention and control mechanisms to keep pace.

According to the United States of America Delegation to the Intergovernmental Expert Group (2006), the extent to which information and communication technologies are available in commercial banks and the extent of their utilization for banking purposes are encouraging. The delegation stated that the modern fraud control and prevention systems are widely utilized in most commercial banks, both in the rural and urban areas. However, Okeke (2007) stated that commercial banks in Nigeria are weak especially in financial security innovation in the market. He also stated that financial security requires

a level of complexity and sophistication, which financial markets in Nigeria do not have. He further stated that emphasis on fraud control and prevention in most cases is mismatch with little success because the quality of corporate governance is still low.

Ning (2007) stated that commercial banks have introduced the on-line verification systems as an important measure to implement the uses of real name for bank account transactions. He stated that the system consists of core parts, namely the systems for information transmitting and sharing. He also stated that the on-line verification systems provide such services as single verification, batch verification; log inquiry, statistics and analysis. Ning stated that most commercial banks are connected to the system.

According to Ning (2007) the on-line verification refers to the process in which a bank verifies a customer's identity, ID Number, photograph, issuing authority and other information as used in the ID card. He stated that commercial banks verify the customers' identity when offering the following products and services: account opening, payment or settlement business, lending service, cash deposit and withdrawal. He further stated that commercial banks have formulated measures for handling the on-line verification and have trained their staff at the basic level so as to make it effective.

The United States General Account Office, GAO (2002) stated that associations that are jointly owned by many commercial banks provide computer systems that transfer data between banks. The GAO stated that the associations establish operating standards that define the policies, roles and responsibilities of the member banks in the use of the data to fight fraudulent

activities. The office also stated that the member banks maintain all account information of their customers. The banks use the data obtained by this cooperation to screen applications through automated systems, for unusual or out-of-pattern transactions.

Usman (2004) stated that some commercial banks have grown into very large organizations but their fraud control and prevention systems have failed to keep pace with their increased scale of operations. He also stated that some banks develop weakness overtime due to work methods that do not meet the best practice. He further stated that a commercial bank's fraud control and prevention systems in general should be regularly and carefully reviewed and maintained to ensure that weaknesses are minimized. Usman also stated that an aspect of commercial banks' fraud control system is the degree to which the management is held accountable for their actions. He stated that if the manager is not accountable for the money he spends, the organization is not likely to prevent or detect fraudulent activities. The activities of the manager and other people in the organization should also be regulated by higher authorities to ensure that accounts are truthfully presented.

According to Smith (1999), the strategies for the prevention and control of fraudulent activities rely to varying degrees upon the actions of people as well as technology. He stated that where the strategies are fully implemented, their benefits in terms of fraud reduction could be predominant. He further stated that the challenge lies not only on identifying and publicizing the strategies but also in their implementation by members of an organization. He also stated that once fraud control policies have been established it is necessary

for them to be implemented and, most importantly, monitored in order to ensure that they achieve the desired effects. The essence of the monitoring project, according to him, is to establish the extent of utilization and effectiveness of the fraud control and prevention systems introduced.

Charlton and Taylor (2004) stated that the techniques used by commercial banks to verify on-line transactions are many. They stated that they include: phoning the customers, checking the customers' records, e-mailing the customers and checking the good and bad customers' database. They also stated that the banks use both manual and automated systems for fraud control, prevention and detection. They further stated that the utilization of some fraud prevention techniques were more popular in some banks than others. According to them, some anti fraud techniques are only applied by some banks after frauds have been experienced rather than as pre-emptive measure. Shackell (2000) then stated that most banks' policies in respect of corporate fraud control, confidentiality, information security, personnel screening, etc remain inadequate when applied against the fraud risks. He therefore, stated that care should be taken by the management of commercial banks to make sure that fraud policies put in place are adequately publicized and enforced as fraud prevention measures.

According to the Bank of Netherlands (2004), the application of computer and telecommunication technologies for corporate fraud prevention is a wide spread phenomenon in financial industries including commercial banks. The banks stated that the trend towards increasing automation is likely to continue for many years to come. The Bank further stated that the success of

the user banks would depend, to a considerable degree, on the quality of the computer and telecommunication systems and the extent to which they develop these systems to match with the evolving views of their business by customers. It was further stated by the Bank that deficiencies in security and control procedures within those systems could pose a significant threat to the continuity of their operations.

According to Mauria (2001), having adequate control systems and maintaining them is a major step in the prevention of frauds but it is not still enough without proper utilization of the systems. She stated that even within the best of systems and their maintenance, all the possibilities of their misuse could neither be predicted nor tested. She further stated that it is very much important to log them, investigate them and finally remove the gaps by suitable modifications in software and /or controls. To prevent fraud, according to her, all events that can lead to system misuse should be properly logged, enquired, investigated into and necessary modifications carried out and patches applied to all places. She stated that event logging, monitoring and auditing are important tools in the prevention of corporate frauds. When the best access control tools are used and monitored, and data flows from within the network through data communication lines or from one network to another or through the internet, protection of data becomes an important tool for the prevention and control of frauds.

Uwakwe (2003) stated that most of the commercial banks have in place many of the modern corporate fraud control and prevention systems. He also stated that most of the banks have competent and trustworthy personnel and

ensure segregation of duties. He further stated that majority of the banks emphasise proper procedures for authorization of transactions. All the banks are now on-line and operate real-time electronic banking services. However, he stated that internal controls are not strictly followed in some banks, and that authority and responsibilities are most times mismatched. He therefore, stated that commercial banks should pay more attention to internal control systems for effective corporate fraud control and prevention.

According to 3VR security Inc (2006), commercial banks have had a head start in managing corporate frauds. The corporation stated that effective fraud prevention systems require real-time testing capabilities backed by databases of identities and accurate views on activities across long periods of time and geographically distributed branches. The corporation also stated that information must be shared between the bank branches and other organizations to prevent repeat frauds from offenders. According to the corporation, when an incident occurs investigators must be able to go beyond a single identity which may appear to be clean to uncover any links of nefarious individuals or groups. The corporation also stated that business and market efficiency require commercial banks to provide customers with immediate access to services. Combating bank fraud actively requires a solution that maintains the openness required to perform business while covertly identifies key threats and enables immediate notification of threats.

- **Effects of Corporate Fraud Control and Prevention Systems Utilized in Commercial Banks**

Corporate fraud control and prevention systems utilized in commercial banks aim at maximizing fraud reduction without imposing unrealistic burdens

on legitimate business activities. Some fraud control and prevention systems may be totally effective in terms of reducing fraudulent activities but may have the consequences of stifling commerce and making everyday business transactions unwieldy and costly to manage that no one would be willing to use them (Smith, 1999). Damagun (2003) stated that to ensure effectiveness, corporate fraud control and prevention systems should provide for the following: authorization of transactions, proper documentation and classification of transactions, separation of duties and supervision.

According to Jenfa (2002), fraud control measures should be effective if they show that the chances of fraudsters being caught or deterred are very high. Jenfa stated that effective fraud control measures in commercial banks should ensure well-fortified vaults and saves, strategic location of information control units, effective supervision and properly defined policies and procedures that are documented and regularly reviewed. He also stated that such fraud control and prevention measures should be able to provide adequate surveillance of customers and staff, restrict the use of specialized equipment and machines to only authorized responsible staff. He further stated that for the control and prevention measures to be effective they should not allow all security measures to be documented.

American Institute of certified public Accountants, AICPA (2002) stated that the most effective way to implement measures to reduce wrongdoing is to base them on a set of core values that are embraced by all in an entity. The Institute stated that the cornerstone of an effective anti-fraud program is a culture with a strong value system founded on integrity. This value system is often reflected in a code of conduct of an entity. The code of conduct should

reflect the core values of the entity and guide employees in making appropriate decision during their workdays. According to the AICPA, the code of conduct might include such topics as ethics, confidentiality, conflicts of interest, intellectual property, sexual harassment and fraud. The code should be developed in participatory and positive manner that will result in both management and employees taking ownership of its contents. The code of conduct should be included in an employee handbook or policy manual or in some other formal documents so that it can be referred to when needed.

According to AICPA (2002) corporate frauds occur less frequently when employees have positive feelings or perception about an organization than when they feel abused, threatened or ignored. AICPA stated that without a positive work place environment, there are more opportunities for poor employee morale, which can affect an employee's attitude about committing fraud against the organization. It also stated that the employees should be empowered to help create positive work place environment and to support the organizations' values and code of conduct. Management needs to clearly articulate that every employee will be held accountable to actions of his within the stipulations of the organizations code of conduct.

Ohazuluike (2001) stated that many factors are considered when reviewing for the effectiveness of fraud control and prevention systems in a commercial bank. Some of the factors, according to him, are: whether the actions of the executives are in consonance with the established corporate policies and procedures, whether there is enough evidence of bank transactions conducted, and whether the procedures and methods are completed as stipulated in the control system? Ohazuluike also stated that consideration

should also be given to whether all transactions are done according to the bank policies, practices and ethics. He further stated that it is also important to ascertain if the innovations are introduced in the best interest of the banks and whether any bottlenecks jeopardize the banks operations. According to him, the effectiveness of corporate fraud control and prevention systems should include the ability of the systems to safeguard assets, confirm liabilities, reduce waste, deter occurrence of fraud and its cost-effectiveness.

According to Farrell and Franco (1999), corporate fraud control and prevention systems are effective when the management of a business, the external auditor and all employees of the business exert concerted efforts towards corporate fraud reduction. They stated that everybody must realize that corporate fraud is not a victimless crime and that the cost of corporate fraud is shared by all through higher costs and lower corporate profits. They further stated that through adequate internal controls by management, better working conditions for employees and more stringent requirements for external auditors, and codes of ethics for employees the fraud control measures can be effective.

Wells Fargo Bank (2003) stated that corporate fraud fighting techniques are only worthwhile if they stay one step ahead of the criminal. The Bank also stated that to control and manage corporate fraud effectively, the management of an organization needed to carefully evaluate the techniques and services available. According to the Bank, effective fraud control and prevention systems lower the time cost of transactions while acting as insurance against catastrophic fraud outbreaks that have brought about the downfall of many growing and stable business organizations. The Bank stated that business organizations with higher fraud risks must be able to make a build or buy

decision to determine if they can battle corporate frauds on their own or if experts' services would be most effective. Effective fraud prevention can be time consuming and complex yet business organizations must process their Internet and other transactions rapidly and cost- effectively in order to prosper.

Graycar (2004) stated that the foundation of an effective fraud control and prevention system is a management that is sensitive to fraud risks. The basic elements of such a system are careful recruitment of staff, a culture of integrity and loss prevention within an organization, and regular auditing of transactions by internal auditor backed up by independent and accountable external auditors. According to Graycar, the first line of defence against complex corporate fraud is to ensure the greatest possible transparency of corporate transactions. He stated that it is widely accepted that effective fraud prevention strategies must, in the first instance, be generated from upper level management. He also stated that if the chief executive officers and managers at all levels have the commitment to corporate frauds prevention and understand how it can be achieved, other employees would support the motions for corporate fraud control and prevention.

Charlton and Taylor (2004) stated that the effectiveness of commercial banks' corporate fraud control and prevention systems depends on the perception and attitudes of the bank customers and staff. They stated that if commercial banks only become aware of their liabilities for on-line fraud after experiencing such fraud and if the delays in the notification of the fraud are substantial, the customers' perception and attitudes toward their banks are negatively affected. They further stated that on-line banking customers usually

believed their banks to be helpful when they have query about accepting payment orders on-line.

Aguolu (2002) stated that to increase the effectiveness of bank fraud control and prevention systems, the staff of banks should have direct access and freedom to report to the top management and where necessary to board of directors and other committees. He stated that the limitations of the effectiveness of the control systems include staff and third party collusions and abuse of authority. Management over-riding of established controls, staff incompetence, alteration of the systems and obsolescence also pose some limitations.

According to Ossai (2005), the effectiveness of the corporate fraud prevention systems depends on the competence and dependability of the people using the systems. He stated that the blame for ineffectiveness of the fraud prevention systems should not be put only on the system but also on human inadequacies. He further stated that the fraud control and prevention systems alone cannot prevent fraud masterminded and executed by management. By the same token, he stated that the systems cannot stop frauds carried out by collusions of staff, management and third parties. The fraud control systems available must be fully utilized by the people to be able to reduce fraudulent activities in an organization.

Reviere (2004) stated that the effectiveness factors for fraud control systems are the improved organizational output, goals, operating skills, systems' resource and processes. He stated that the control systems are effective if they can achieve the stated goals, acquire needed resources and inputs, smooth processes and produce high outputs. He further stated that the

systems could be effective if they can deal with environmental and technological changes and internal barriers. According Reviere, the systems are said to be useful and effective if the goals are clear, concessionary, time borne and measurable. There should also be clear relationship between input and output, processes and outcome. The survival and downfall of the systems can be assessed and the demands of the organization are compressible and cannot be ignored if the systems are effective.

Reviere (2004) then stated that the effectiveness of corporate fraud control and prevention systems is attained when all the systems succeed in controlling fraud according their abilities. Effectiveness is not just linked to the systems ability to eradicate fraud but its ability to reduce and minimize the occurrence of fraudulent activities. That is the ability of the systems to produce the desired results or outcomes.

According to KPMG (2006), an important part of an effective fraud control and prevention strategy is the use of due diligence in the hiring, retention, promotion of employees, agents, vendors and other third parties. Such due diligence may be especially important for those employees identified as having authority over the financial reporting process. KPMG stated that due diligence begins at the start of the employment or business relationship and continues throughout taking into account behavioural considerations. The behavioural considerations include adherence to the organizations core values in performance evaluations. Due diligence should provide a powerful signal that management cares about not only what employees achieve but also that those achievements were made in a manner consistent with the organization's values and standards.

The evaluation of the corporate fraud control and prevention systems' effectiveness, according to KPMG (2006), should focus on the extent to which the systems' objectives have been achieved. For example, have the mitigating strategies identified during the fraud risk assessment been implemented properly? Similarly, management may have put in place a well-designed code of conduct, but are employees actually using the code to guide their day-to-day activities? KPMG stated that in the end, integrity climate would determine the perceptions employees have on the ability of the organizations to prevent, detect and respond to fraud and misconduct and base their own conduct on those perceptions. KPMG further stated that only when such basic questions are addressed can management focus on gathering empirical data on control effectiveness using review and evaluation techniques e.g. proactive forensic data.

Nduka (2001) identified the prerequisites for effective fraud control system. They include the following: (a) Obedience to rules and regulations by everyone in the organization (b) efficient and trained persons to execute the jobs in the organization (c) a good organization chart with chain of command and adequate span of control for effective performance and (d) adequate remuneration of staff. Nduka stated that the organization's ethics and code of conducts should be enforced and obeyed by all for the fraud control systems to be effective. He further stated that effort should be made to see that the personality potentials of staff are emphasized rather than focusing only on academic capacity. He also stated that the management of commercial banks should ensure the management of controls that should be complied with by all staff and other people who have stakes in the banks.

Anxciom and Transunion (2004) identified the variables to be looked for in effective fraud control and prevention systems. The variables include: system flexibility, open access and integration, true analysis, multi-sourced data, processing options, breadth of data sources, fraud risk analysis and recognized leader. They stated that fraud patterns tend to change and fraud prevention solutions should adapt to those changes. They also stated that the ability of the solution to look to variety of infrequently updated databases and calculate different scores without costly updates is critical to an effective fraud prevention measure. They further stated that a prevention measure must be able to integrate easily into existing financial systems while remaining open to further data input. As new data sources become available and financial systems change, the fraud prevention systems must be able to access new data while integrating with the new systems.

The fraud prevention and control systems, according to Anxciom and Transunion (2004) should objectively determine what constitutes fraud rather than relying on error prone subjective scoring. The systems should provide a variety of options for producing fraud score, ranging from real-time to overnight operations. The systems should be able to examine and analyse many sources to provide the true picture of a person's identity. The solutions should also be able to work with recognized leaders in fraud prevention and control. They stated that these leaders often offer one-stop solutions for verification, authentication and compliance requirements making it easier to implement and maintain the systems.

According to Okereke (2000), no fraud control and prevention systems can guarantee total fraud control and prevention. He stated that the

effectiveness of the systems could be limited by such variables as incompetence of staff, lack of integrity, fatigue, human error and the alteration of the system by staff for their own considered improvement. He further stated that the effectiveness of a fraud control system could be ensured if authorization control is not abused and segregation of duties is not avoided by collusion of management and employees or with third parties.

- **The Problems Encountered by Commercial Banks in the Utilization of Corporate Fraud Control and Prevention Systems**

Commercial banks are faced with many problems in the course of utilizing corporate fraud control and prevention systems for banking operations. Some of the problems faced by the banks are collusion of bank officials and third parties, abuse of security, over-ride of control measures by management, poor remuneration of staff and poor working conditions of employees (Adeniji, 2004). Adeniji stated that commercial banks have the problems of making sure that the cost of the fraud prevention systems utilized are not higher than the potential cost that can accrue from not establishing or utilizing those systems. Other problems faced by commercial banks in the utilization of the fraud control and prevention systems, according to Adeniji, are potential human errors caused by heavy work load, carelessness, distraction, poor judgment, misunderstanding of instructions and lack of initiative.

Anyafo (2004) identified many problems faced by commercial banks in their anti-fraud programmes. The problems, according to him, include: unsound lending policies, inadequate operational manual, bad management and staff infidelity, poor condition of service of staff and general indiscipline in the work

environment. He stated that inadequate knowledge and training of staff, lack of appropriate sanctions for offenders and other shortcomings of both the bank staff and management negatively affect the effective implementation of corporate fraud prevention systems in commercial banks.

Usman (2004) stated that over-ride of control measures by mangers, collusion between bank employees, customers and third parties, lack of accountability, poor ethical culture and poor hiring of employees are problems encountered by commercial banks while utilizing the fraud control measures. He also stated that problems may occur involving a manager "cutting corners" when processing transactions especially by dominant management personnel. He further stated that unscrupulous customers and third parties might offer inducement to staff in attempt to involve them in achieving their fraudulent aims. He stated that once such a relationship is established, the employee could help to facilitate the fraudulent activity by skipping the fraud controls and prevention strategies available. This tendency is frequently experienced, according to him, where the ethical culture, staff recruitment practices and promotions are poor.

According to Wells (2004), one of the most difficult problems facing banks in the utilization of fraud control and prevention systems is that there is no one control or prevention procedure that provides absolute assurance for corporate fraud control. For instance, he stated that no auditing procedure provides absolute proof for fraud financial reporting. He further stated that as a result auditors have continually attempted to avoid, albeit unsuccessfully, the responsibility of fraud detection. He also stated that the expectation the public

holds for auditors in respect to fraud detection simply could not be fulfilled. Wells (2004) identified other problems faced by banks in the utilization of the fraud control and prevention systems to include the perception of staff, customer and the general public on the banks' efforts towards fraud prevention and control. Others are the financial condition of some banks and the pressure to show profit in their published accounts. This problem is especially encountered with systems that are costly both in establishment and in enforcement. The organizational culture and ethics together with the dynamism of commercial banking also pose limitation to fraud control and prevention.

Okereke (2000) stated that no fraud control system could by itself guarantee effective fraud control. He stated also that no fraud control system could be a proof against fraud collusion especially on the part of those holding positions of authority or trust. He further stated that fraud control measures that depend on segregation of duties could be avoided by collusion of bank staff and management. The person who the authority is vested on can also abuse authorization control. He stated that the effective implementation of corporate fraud control and prevention systems could be limited by such factors like incompetence, lack of integrity, fatigue, human errors and the alteration of the systems for the operator's own considered improvement.

Linnitt (2006) stated that the problem faced by commercial banks in credit card fraud control and prevention is that the security of the card information is reliant on the banks' own protocols, systems and general security level and not that of the card issuing company. He also stated that many banks can share facilities and hence any bank will be able to process the

credit transactions on cards issued by another bank. This means, according to him, that such transactions are entrusted to the processes and protocols of yet another bank and not the issuing bank. It becomes a problem since the responsibility for and the duty of care to the cards actually falls on the issuing bank. He stated that the problems on the issuing banks is pathetic because when a customer incurs a loss due to credit card fraud, the credit card company underwrites it but reclaims the money from the issuing bank. This, according to Linnitt, is because the credit card bears the symbol of a company that controls and regulates it while a bank that is required to meet the standards set by the company issues the card to her customers.

Kama(2003) identified many constraints to effective supervision and surveillance of corporate fraud control and prevention systems in commercial banks. Some of the constraints are unprofessional and unethical practices among the management and staff of banks. He stated that lack of transparency in dealing with regulation often reflect in the rendition of false or unreliable returns and non-compliance with existing laws, guidelines and circulars. He further stated that inadequate capacity building; inadequate legal framework and poor corporate governance on the part of the bank operators also affect the level of utilization of the anti-fraud systems. Another constraint, according to Kama (2003), is the inability of regulators and some operators to cope with the pace of technological innovations. The problems are also attributed to lack of proper understanding of what regulations and systems are all about. Lack of adequate information on the part of the customers and banks about some modern corporate fraud control and prevention systems also pose problems to them during the implementation stage of the systems.

According to Osasebor (2004), increasing workforce mobility among bank staff means that corporate information systems and security knowledge are no longer restricted to employees within the bank but also held by people external to the bank. This, according to him, poses definite challenges to the fraud control and prevention programmes. This is especially true for the monitoring and evaluation of the systems and their operators. Osasebor stated that this vulnerability requires constant management consideration and review to ensure the effectiveness and efficiency of the systems.

Jenfa (2002) stated that the institutional factors that affect the systems include inadequate training and retraining of staff on both technical and theoretical aspects of the systems. According to Jenta, failure by both the management and staff to undergo on-the-job training and even relevant outside courses lead to unsatisfactory performance which eventually creates more room for malpractices. He stated that malpractice and error occur with higher frequency among staff with little experience and knowledge about the systems. He further stated that the use of sophisticated accounting machines could be employed by dishonest staff to deliberately omit entries, substitute it with improper calculation and manipulate documents unduly to substitute genuine entries with fictitious ones.

Smith (1999) stated that most of the fraud control systems available are unlikely to be taken up fully by banks because of the costs involved and the perceived potential impact on commerce. He stated that some artificial boundaries exist between public and private sector agencies and between these agencies and individuals in the communities, which can affect fraud prevention

and control. These boundaries, according to him, need to be removed to enable them act cooperatively within specified framework for fraud control and prevention.

According to Vittal (1999), computer programmes used for fraud prevention are often highly complex containing typically thousands of lines of computer coding, which may contain errors. He stated that while these programs may have been well tested, a risk still exists that errors can remain in-active and dormant for a long time. The errors only appear when certain set of circumstances occurs. Vittal stated that standard software packages are also not immunized from errors which may occur when the packages are "Customized'' by the vendor and adapted to a particular bank. He also stated that particular risks are also associated with the implementation of new systems and all the security requirements of a new system should be considered prior to a system being specified or designed. He further stated that if this exercise does not take place, the bank is at the risk of the new systems being unreliable and difficult to secure against unauthorized access and activities.

According to Vittal (1999), as banks also become increasingly computerized, their ability to operate for any significant length of time without the computer and telecommunication systems falls. The commercial banks are ultimately reliant upon a number of components that together make up the banks' technical infrastructures. These components include: quality operational and management staff, power supply, healthy communication and telecommunication systems, effective security network, etc. An absence of any of these can bring the fraud prevention systems down. This could be in an

unexpected or planned event occurring. Vittal stated that the impact of a discontinuity or bad operation of the computerized systems could be dramatic. According to him, processing backlogs can build up which can take hours or even days to process and where ATMs are being used, the impact on the customer will be almost immediate. He stated that if computer facilities and related infrastructures are not adequately protected, the result might be a major impact upon the continuity and even the going concern of banking operations. Inadequate continuity arrangements may result in a loss of business, damaged reputation and loss of assets.

Ngige (1999) stated that often the operation of the fraud control and prevention systems are in the hands of people who are not too skilled in the act. The people, according to him, are often victims of incessant mistakes and busy themselves with the rectifying of mistakes instead of developing initiatives and innovations. He stated that sometimes employees employed to operate the systems are not skilled and educated about the job. He further stated that staff and customers constantly need to be educated, trained and retrained for operating fraud control and prevention systems.

Cole and Cumming (1998) identified poor management oversight and control culture, inadequate risk recognition and assessment, and failure to observe key fraud control principles as problems faced by banks in the utilization of anti-fraud systems. They stated that the problems also include misinformation, inadequate lines of communication and poor monitoring of activities. They also stated that some commercial banks have the problems of not clearly defined organizational structures and accountabilities. Failure to

update the risk management processes by bank management as the operating environment and transactions change also affect the effective implementation of the fraud control systems.

According to smith (1998), the cost and volume of data required on-line to ensure proper identification of customers is, however, prohibitive. He stated that there is always the possibility that computer security systems could be compromised by reproducing data streams which correspond with the biometric characteristics of the customers or even a fraudulent person seeking bank services. He also stated that some people find the process of providing personal information in public distasteful which is one of the reasons given for the reluctance of some customers to make use of cheque fraud prevention initiative that requires customers to leave their finger prints on cheques. Smith further stated that maintaining expensive databases of individuals is another way of being able to validate identities. However, he stated that this raises the problems relating to privacy and security. He also stated that some customers could submit documents that have been forged or altered through the use of computerized desktop publishing equipment.

The main problem, according to smith (1998), with having so many security features in plastic cards for fraud prevention is that those who are required to validate them might not be familiar with all the features present in the legitimate card. Often, the people are not trained on how to recognize counterfeit copies. Smith also stated that there is also the possibility of bank staff being subjected to intimidation or violence if they refuse to process transactions or delay unduly.

- **Strategies for Enhancing the Effective Utilization of Corporate Fraud Control and Prevention Systems in Commercial Banks**

Quova Inc. (2005) discussed how to improve the effectiveness of fraud control and prevention systems utilized in commercial in banks. According to Quova, to improve on the effective utilization of fraud prevention and control systems, bank employees should be taught how to spot false identification, counterfeit currency, fraudulent cheques and other indicators of criminal activities through a combination of experience, awareness and education. The online banking services for fraud scoring and authentication systems currently in place at commercial banks require updating with new techniques based on the changing trends and behaviours detected on the Internet. Quova (2005) also stated that online banking services have protected themselves from unauthorized access with personal procedures, usually involving a customer sign-in process employing various combinations of account number, social security numbers and encrypted passwords.

Zervos (1999) noted that the methods of dealing with the problems of frauds have been inadequate, and neither responsive nor effective. He stated that organizations should aim at responding to fraud with the same dedication, sophistication and agility with which it operates. He stated that for organizations to meet these objectives it is imperative that organizations have the appropriate structures in place. These would include programmes for staff training, fraud awareness and education for employees and other stakeholders. He further stated that there must be a committed and continuing programme of monitoring and controlling the problem, and where necessary anticipating and focusing upon new programmes and recommending changes in structures,

systems, work practices and procedures. Zervos (1999) stated that formal studies, critical examination of existing systems and procedures for the purpose of identifying weaknesses and recommending methods of improvement is very important. According to him, fresh approach with fresh ideas needs to be employed in the fight against corporate fraud. New approaches and additional or new roles should be considered and assumed about the pattern of behaviours of people in organizations to improve on effective fraud control and prevention. Innovative and broad-based approaches are required to respond to the problems of corporate fraud.

American Institute of Certified Public Accountants, AICPA (2002) stated that research suggests that the most effective way to implement measures to reduce wrongdoing is to base them on a set of core values that are embraced by all in an organization. These values should provide an over-reaching message about the key principles guiding all employees' actions. This provides a platform upon which a more detailed code of conduct can be constructed, giving more specific guidance about permitted and prohibited behaviours based on applicable laws and the organization's values. Management needs to articulate that all employees will be held accountable to act within the organization's code of conduct. The Institute stated that corporate fraud mitigating factors should be highly promoted in an organization including commercial banks. Some of them are equal employment opportunities, team-oriented collaborative decision-making policies and professionally administered compensation programme. Others are professionally administered training programme and organization's priority for career development.

Recognition of and the use of reward systems that are in conjunction with organizational goals and results are also included.

Uwakwe (2003) outlined the principles that should be followed by organizations to improve their fraud defences. They are: recruitment of competent and responsible employees, separation of duties, rotation of duties, establishment of effective corporate rules and regulations to control the human, material and financial resources of an organization. Others are well-designed source documents, internal auditing and adequate financing of risk analysis, and other exposures in the organization. They should also be regular and frequent regulatory examination of assets, finances, records and systems in the organization. He also stated that there should be continuous professional development and training for staff and management personnel. The internal audit department should also be adequately staffed and monitored.

Ossai (2005) recommended that commercial banks should conduct or sponsor employees to attend specialized seminars and workshops on fraud control and prevention. He stated that there should be regular, unannounced and independent check on staff and their operations. Bank employees should be sent on professional training and refresher courses on regular basis. Banks should provide enough and commensurate incentives and motivations to employees who stand out in their work activities.

Ngige (1999) stated that computer frauds in banks like any other risk that threatens commercial banks has to be identified, measured and controlled. The practical approach, according to him, should begin with computer security and audit conducted by a competent professional. He stated that extensive

training and orientation in the effective use of online systems should be an imperative for staff of commercial banks.

Itukwe (1998) recommended that corporate fraud management could be improved by increasing the staff strength and recruitment of professionals in banks' personnel departments. He stated that there should be improvement in research and development about the current techniques for fraud control and prevention. Adequate social and job security initiatives should be maintained together with improved reward systems to staff that excel in their jobs.

Wilhelm (2005) stated that in order to implement an efficient system of fraud control and prevention within a company, motivational power, as an internal means of influence must be used to make employees comply with ethical standards. Motivational power must be used to help them regain a sense of purpose and mission. This is to let them become emotionally attached to their company. Wilhelm stated that this would help employees to move towards ideological and personalized internal coalition. The success of trusted control to prevent fraud, according to him, depends on the ability to adapt to performance measurement systems to include ethical behaviour and actions to prevent fraud. Since external stakeholders have only limited access to internal means of influence, the effectiveness of a fraud prevention system relies on the willingness and capability of corporate management to skillfully apply internal means of influence for corporate fraud prevention. He further stated that trusted control appears to be an indispensable component of effective fraud prevention. He observed that corporate fraud could only be prevented effectively if control efforts are firmly rooted in both external and internal means of influence. The

critical success factor will be to win the full support of the internal coalition for fighting fraud uncompromisingly.

Smith (1999) stated that some fraud control and prevention strategies that have proved successful might not likely be taken up fully because of the costs involved or the perceived potential impact on commerce. He stated that special funds should be provided for their acquisition and implementation while the less costly ones that are effective should generally be utilized in the organization. He further stated that organizational budgets should specifically provide much funds for the installation and utilization of fraud control and prevention systems; provision of other infrastructures like alternative power supply and the training of employees and management personnel for the effective implementation of the acquired systems. Smith observed that the provision of information and communication technologies, which are less expensive and are likely to yield greatest immediate benefits in terms of fraud prevention, should be pursued vigorously. He also stated that in preventing corporate frauds, it is essential that those involved should work cooperatively, making use of the latest developments devised to deal with the sometimes highly specific and deviously imaginative ways in which corporate fraud is now being perpetrated.

Vittal (1999) recommended that the design and operation of banks and their computer systems must reflect and comply with the regulatory framework in place. He stated that the organizational structure of commercial banks should provide and clearly define reporting lines and responsibilities for organisational functions. The banks data processing equipment should be strategically located to reduce unwanted access to them. He further observed that adequate training

should be given to operators of these systems to make business strategies more effective in line with technological realities. Commercial banks should adopt simultaneous tight and loose policies to manage the systems. They should also consider fraud control and prevention systems' capacity when making products decisions. They should also get rid of huge share cost structures and provide enough funds for the acquisition of and utilization of the current techniques and systems for corporate fraud control and prevention.

Ugwunna (1998) stated that employees skilled and educated in the use of the modern techniques for corporate fraud control and prevention should be assigned to operate the systems. He also stated that in-service training and refresher courses should be regularly conducted for both staff and management of commercial banks. Fraud control and prevention systems should always be revitalized through regular reviews and examinations. Staff and customers should always be informed and educated on the need and use of available fraud control and prevention systems in the banks.

Farrel and Franco (1999) stated that concerted efforts must be exerted by management of the business, the external auditors, and by all employees to effectively combat corporate frauds in an organization. According to them, this can be achieved through adequate internal controls by management, better working environments for employees, more stringent requirements for external auditors and codes of ethics for employees. They stated that when a control has been for a designated period of time, it should be evaluated to determine its ability to achieve the optimal effectiveness it was designed and implemented for. When evaluating the design effectiveness of a fraud control or prevention system, according to them, management should take into account both

regulatory requirements and leading practices that similarly situated organizations have found to correlate with effective risk mitigation.

Theoretical Framework

A number of theories has been identified which help to lay the foundation of this work. Weber's theory of bureaucratic management propounded in 1947 is a classic example. The theory deals with an individual's obedience to legitimate authority. It stipulates that bureaucracy is the most appropriate and efficient way of managing large organisations. Bureaucracy, according to the theory is characterized by division of labour and a clear hierarchical authority structure. It also calls for formal and unbiased selection procedures and employment decisions based on merit, detailed rules and regulations. It also entails uniformity in the application of rules, impersonal relationships, and distinct separation of organisation and personal lives.

This theory believes in the standardization of rules and obedience to the rules and procedures for effective attainment of organisational goals as well as the security of persons and property. Organisations are viewed by this theory as being concerned almost entirely with control mechanisms by emphasizing formal activities, rules, regulations and designation of formal positions. The chief merit of bureaucracy is its technical efficiency for organisational effectiveness with premium placed on precision, speed, effective control system and continuity of the organisation. Effective application of the principles of this theory reduces vulnerability and threats to both lives and property in the organisations. The controlling practices in most commercial banks in Nigeria are based on Weber's theory of bureaucratic management. For

instance, the use of written operational procedure manual and employment screening procedure as well as method of posting, placement and disengagement of staff for corporate fraud control in commercial banks in Nigeria is based on Weber's theory of bureaucratic management.

Similarly, Mintzberg (1983) developed the theory of trusted control. In this theory, trusted managers retain control power because they are socially responsive and exercise power responsibly. In order to implement an effective and efficient system of trusted control within an organisation, motivational power must be used to make employees adhere to ethical standards in their daily lives. Furthermore, motivational power helps them to regain a sense of purpose and mission, and make them emotionally attached to the organisation. The theory is very important for management because there is always some degree of discretion available to managers when decisions are made. Trusted managers usually use their discretional power when taking decisions about unethical behaviour, fraudulent opportunities and even behaviours that contradict rules and regulations in the organisations. The effectiveness of trusted control relies on the willingness and capability of corporate management to skillfully apply motivational power to fight fraudulent activities in the organisations. This theory is grounded in motivational techniques that achieve organisational goals. In return, the manager wins employees' obedience in fraud reduction and avoidance in the organisation. Trusted control is an indispensable component of an effective fraud control and prevention system when adopted by managers in modern organisations.

Mayo in 1933 propounded the human relations theory. This theory describes an organisation as a social system encompassing individuals, informal groups and intergroup relationships as well as formal structures. Organisations are reorganized to include informal structures and norms as well as formal practices. Employees create informal rules, patterns of behaviour and communication, norms and friendship to meet their emotional needs. The theory stipulates that social factors can have more influence on individual behaviour and performance than formal structures. People seek to meet their emotional needs through the formation of informal but influential workplace social groups. People are considered to be emotional rather than economic rational beings. Employees are not solely motivated by money, but by being accepted as human beings.

The individuals' emotional and social needs can have more influence on their behaviour at work than financial incentives. The workers' performance and attitude are influenced more by their need for security and also by feeling of belonging to the informal groups. The management of modern organisations becomes conscious of the effect of organisational structures and job design on workers. The success and effectiveness of modern organisations including commercial banks are based on the of Mayo's theory of human relations. The controlling practices of reaching out to people and conveying management ideas to employees through various group relationships in modern commercial banks are based on Mayo's theory of human relations.

Koontz et al (1972) propounded the theory of staff discipline and control. This theory is concerned with how much the employees of an

organisation are ready to comply with the rules and regulations governing the conduct of the organisation. This theory is interested in the ability of the employees to remain within the bounds of the rules defined by the organization. The theory measures how the employees comply with the rules. The control is concerned with the ability of the organisation to pursue and attain its intended objectives by using its human resources. The willingness of the employees to comply with the rules and regulations set by the organisation is largely dependent on the response of the organisation to the actions of its employees. Managers of modern organisations use appropriate reward systems to encourage the employees that comply with the rules. Employees that behave contrary to the rules are punished to discourage others from disobeying the rules in the organizations. The control practices of personnel administration witnessed in many commercial banks in Nigeria today are based on Koontz theory of staff discipline and control.

Furthermore, Fayol (1949) propounded the theory of controlling principles for achieving security in an organisation. He grouped all the organisation activities into six of which security is one of them. According to him, security pertains to the protection of property and persons in the organisation. Security can be achieved by setting a standard for all activities and what is acceptable should be defined as early as possible for all tasks including security. Setting the standard is useless unless actual performance is measured and compared against the standard of measurement. The measurement may take many forms but regardless of the method taken, an activity should be regularly evaluated. Fayol stipulated that when the measurement of performance indicates that a standard is not being met

appropriate corrective action should be taken. Failure to correct what is wrong leads to waste of human and material resources. The waste of resources can be reduced through proper division of work processes, observance of authority, responsibility and accountability procedures. The waste of resources can also be reduced through the motivated and disciplined employees.

The effective management of modern organisations is rooted in the above theory. Modern organisations regularly review and evaluate the control measures introduced in their organizations. This is to ensure that organisational properties and persons are adequately protected. This theory also provides the managers of the organisations with the impetus for systems analysis and control. The need to establish corporate fraud control and prevention systems in commercial banks in Nigeria can be traced to Fayol's theory of controlling principles.

Banard (1938) propounded the theory of cooperative systems of organisations. This theory views an organisation as a cooperative entity for achieving the common goals of all the members of the organisation. The managers of organisations create proper channels of communications to enable the cooperation of members in the attainment of the organisational objectives. Modern managers are usually conscious of the reactions and cooperation of their employees when taking decisions about the rules and regulations in the organisations. Corporate organisations including commercial banks cannot operate effectively without the willingness of their employees to cooperate in the pursuance of the organisational plans and objectives. Corporate managers provide incentives to their employees to achieve the goals of the organisations.

The managers also set clear and realistic goals for their organisational members to pursue through effective communications. Effective communication by all participants in an organisation is an important function of the executives. The current use of modern communication systems by managers of commercial banks in Nigeria to win the cooperation of their employees is rooted on Banard's theory of cooperative systems.

Related Empirical Studies

Considerable empirical studies have been conducted in the area of the present study. Nwofor (2006) conducted a study on fraud and the Nigeria economy (1991-2006). It was a case study of selected commercial banks in Enugu state of Nigeria. The major purpose of the study was to identify and examine the causes, effects and control of bank frauds. The findings of the study were that (a) Bank frauds mostly occur as a result of inadequate internal control, dishonesty of some bank staff and their collaboration with third parties (b) inability of on-line banking to minimize fraud even with the recruitment of qualified staff by banks (c) Frauds reduce the reputation of banks, the confidence and trust the customers repose on them. The present study is related to that of Nwofor in that both focus on the examination of fraud control systems in commercial banks. But Nwofor's study was a case study of selected commercial banks while the present study used descriptive survey design to investigate the corporate fraud control and prevention systems in all commercial banks in Enugu state.

In another related study, Ossai (2005) conducted a study on the effectiveness of internal control in fraud prevention and control in the Nigerian

public sector. It was a case study of the cash-off centre of Delta State University at Abraka. The population of the study comprised all the permanent staff of the cash-off centre. The study adopted descriptive survey design. The major purpose of the study was to ascertain the extent of the effectiveness of internal control in fraud prevention in the public sector. The study found that (i) internal control are not effectively used in the public sector (ii) the effectiveness of internal control is limited by errors of carelessness, misunderstanding of instructions, collusion and over-ride of the controls by staff and management. The study concluded that internal controls are established to help meet an organization's goals especially in fraud reduction. It was also on the conclusion of the study that internal controls consist of specific policies and procedures designed to provide management with reasonable assurance that goals and objectives of the organizations will be met. The present study is related to that of ossai in that both aim to ascertain the effectiveness of fraud control measures. However, while Ossai's study was delimited to the public sector the present study surveyed commercial banks (private sector).

In the same vein, Mbamalu (2004) conducted a study on the management of fraud in Nigerian commercial banks. The study surveyed selected commercial banks in Nnewi. The population of the study was made up of the managers, accountants and supervisors of all the selected commercial banks. The major purpose of the study was to determine the extent of implementation and the effectiveness of anti-fraud management strategies in commercial banks. The study found that the commercial banks established and implemented many fraud control and prevention strategies. The study also

found that some of the strategies were not effective because of their complexity and sophistication together with inadequate qualified staff to operate them. Mbamalu's study is related to the present study because both focus on the extent of implementation and the effectiveness of fraud control systems in commercial banks. However, the present study is delimited to commercial banks in Enugu state while the previous study was on selected commercial banks in Nnewi, Anambra State. The present study also differs from the previous study because it is determining the corporate fraud control and prevention systems in commercial banks in Enugu state.

Similarly, Nduka (2001) conducted a study on the effectiveness of the internal control method as a tool for preventing bank frauds in Nigeria banks. It was a case study of five commercial banks in Enugu. The population of the study comprised all the management staff of the five commercial banks. The management staff were the managers, the accountants and the supervisors in the commercial banks. The major purpose of the study was to determine the effectiveness of internal control methods utilized in commercial banks for fraud control and prevention. The study found that the commercial banks had adequate internal controls but while some controls were effective others were not because of collusion and over-ride of controls by both management and staff of banks. The present study is related to Nduka's study in that both focus on the effectiveness of fraud control systems. However, while Nduka's study was centred on internal control only in five commercial banks, the present study considers the entire corporate fraud control and prevention systems in all the commercial bank branches operating in Enugu State. The present study is

interested in the availability, the extent of utilization and the effectiveness of corporate fraud control and prevention systems in the banks.

Ume (2001) conducted a study on the role of management in fraud control and detection. The study was a comparative study of two public and two private organizations in Enugu. The major purpose of the study was to examine comparatively the role of management in fraud control and detection in public and private establishments. The study found that management in the public and private sectors, respectively, implemented fraud control and detection strategies to achieve the organisational goals. It also found that management in public organisations more frequently manipulate the fraud control measures than those in the private sector. The present study is related to Ume's study in that both focus on fraud control measures adopted by business organisations. However, the present study is not a comparative study but purely on commercial banks, which are in the private sector.

In another study, Nzekwu (1999) conducted an assessment of the manual and computer-aided fraud techniques in Nigerian Banking systems. Nzekwu conducted a case study of Union Bank of Nigeria PLC. The area of the study was Enugu. The study surveyed all the permanent staff of the bank. The major purpose of the study was to evaluate the manual and computer-aided fraud control and prevention techniques used in Nigerian banks to ascertain their effectiveness. The findings of the study include: (a) that both manual and computer-aided fraud control and prevention techniques were utilized in banks but the computer-aided techniques were more effective (b) That some computer-aided techniques were not fully utilized because of the complications

in their operation and shortage of qualified staff to operate them. The present study is related to that of Nzekwu in that both focus on the fraud techniques used in Nigerian banks. But the present study differs from the previous study because it is not a case study on one commercial bank. The present study also differs from the previous study because it is on the corporate fraud control and prevention systems in commercial banks in Enugu state while the previous study was only on the manual and computer-aided techniques.

Furthermore, Ugwunna (1999) conducted a study on fraud in the Nigeria banking industry in Enugu. The major purpose of the study was to determine how accounting controls and procedures were used to minimize fraudulent activities in banks. The study found that most of the banks employed adequate accounting control measures for fraud reduction but because there were misconceptions about the measures, some staff violated and rendered the measures ineffective through collaborations. The present study is related to that of Ugwuna in that both focus on fraud control and prevention in Nigerian banks. But the present study is delimited to the corporate fraud control and prevention systems utilized in commercial banks in Enugu State and not only on the use of accounting controls and procedures to minimise fraudulent activities in banks.

In a similar study, Ngige (1999) examined fraud and its control in banks in Enugu. The study was a critical analysis of computer usage in fraud control in banks in Enugu. The major purpose of the study was to analyse and ascertain the effectiveness of computer-assisted fraud control measures applied by banks. The findings of the study were that (a) the use of computers was not yet very

effective in fraud control and prevention in banks because most times the operation of the computers were in the hands of people who were not well skilled for the act and (b) that the security of the computers was not strictly maintained. The present study is related to that of Ngige in that both aim to ascertain the effectiveness of fraud control measures utilized in banks. However, the present study is not delimited to computer usage for fraud reduction but to all the corporate fraud control and prevention systems in commercial banks in Enugu State.

Kanu (2004) conducted a study on the management of fraud in Nigerian commercial banks. It was a case study of union bank of Nigeria plc. The population of the study comprised the managers, supervisors, internal auditors, accountants and other permanent staff of 15 branches of Union Bank. The study adopted survey research design. The major purpose of the study was to determine the effective ways of reducing the occurrence of frauds in commercial banks in Nigeria. The study found that there was an increase in fraud incidences in commercial banks in Nigeria. The study also found that internal audit and internal control were effective in the reduction of frauds in Nigerian commercial banks. The present study is related to Kanu's study because both focus on the control and prevention of frauds in commercial banks. However, the present study differs from the previous study because it is entirely on the corporate fraud control and prevention systems in all commercial banks in Enugu State while the previous study was a case study of one commercial bank in Nigeria.

Rauta (1992) conducted a study on internal control and fraud prevention in commercial banks operating in plateau state. The population of the study

comprised all the management staff of all the commercial banks in Plateau State. The study adopted survey research design. The major purpose of the study was to ascertain the effectiveness of internal control in commercial banks in Nigeria. The study found that commercial banks had internal control systems but it was not adequate for effective fraud control and prevention. It was also found by the researcher that frauds persist in the commercial banks because of the failure of management and staff of the banks to comply with the internal control systems. The previous study and the present study are related in that both focus on the effectiveness of fraud control in commercial banks. However, the present study differs from the previous study because it is on all the fraud control and prevention systems utilized in commercial banks but the previous study was centered on internal control only. The previous study was on commercial banks in plateau state of Nigeria while the present study is on corporate fraud control and prevention systems in commercial banks in Enugu state of Nigeria.

Similarly, Ohia (1997) conducted a study on internal control and fraud prevention in merchant banks. It was a case study of Stanbic Merchant Bank Nigeria Ltd. 80 bank supervisors and managers were surveyed for the study. The purpose of the study were to ascertain the degree of compliance with laid down procedures of control and to examine the adequacy of internal controls in preventing frauds in the bank. It was found in the study that employee compliance with internal control made the controls effective in fraud prevention. The study also found that there existed adequate internal controls for fraud prevention in the bank. The present study is related to the previous study because both focus on fraud control and prevention. However, while the

previous study was on internal control and fraud prevention, the present study is on corporate fraud control and prevention systems. The present study is on commercial banks in Enugu state while the previous study was a case study of a merchant bank in Nigeria.

Agbo (1991) conducted a study of frauds in the Nigerian banking system. It was a case study of CCB and Union Bank of Nigeria, Enugu. All the permanent staff in the two banks were used for the study. The major purpose of the study was to determine the role of the internal auditor and external auditor in fraud prevention and detection. The purpose also included the role of police and bank examiner in fraud detection and prosecution in banks. It was on the findings of the study that internal audit and external audit were effective in fraud detection and prevention in banks but their roles were not yet comprehensive for significant fraud reduction in the banks studied. The present study is related to the previous study because both focus on the prevention of frauds in commercial banks. However, the present study differs from the previous study because it is studying all the commercial banks operating in Enugu state while the previous study was a case study on two commercial banks in Enugu.

Summary of Review of Related Literature

The review of related literature showed that commercial banks are highly prone to fraudulent activities because of the new payment systems and fund transfers that are organized electronically and on-line. The banks are also vulnerable to frauds because of the huge financial assets handled by them. According to literature, fraud is a category of crime that involves people

dishonestly obtaining property or some financial advantage by deception. Frauds that occur to business organizations are called corporate frauds.

Corporate frauds, as revealed by literature, can be reduced or minimized through robust fraud control systems. These are the various strategies applied by commercial banks for fraud avoidance and fraud minimization. Some of the fraud control measures are careful screening of applicants, fraud awareness and education, personnel and transaction monitoring and personal identification. The authors whose works were reviewed were in agreement that commercial banks establish many barriers to discourage and prevent the occurrence of fraudulent activities. Some of those barriers include: secure management of information, the use of neural networks, electronic payment authorization, biometric identifiers and geolocation of users of the bank services and products. The literature reviewed also indicated that Nigerian commercial banks are fully computerized and operating on a full electronic and online platform.

The authors held the general opinion that the aim of corporate fraud control and prevention systems utilized in commercial banks was the maximization of corporate fraud reduction without imposing unrealistic burden on legitimate business activities. They agreed that some of the fraud control and prevention measures may be totally effective in terms of reducing fraudulent activities but may have the consequences of stifling commerce and making everyday business unwieldy and costly.

The literature also identified many problems encountered by commercial banks in the course of establishing and utilizing the corporate fraud control and prevention systems. The problems include high costs, complexity and

sophistication of the systems. The authors of the literature also suggested some ways of improving the effective utilization of the corporate fraud control and prevention systems in commercial banks

From the theoretical viewpoint, many authors made contributions on how to manage corporate organisations especially for fraud control and prevention. The authors agreed that motivational techniques, bureaucracy and informal structures are important in the management of corporate organisations including commercial banks. It was also seen from the theories reviewed that the cooperation of employees gained through proper channels of communications, formal group and intergroup relationships are vital in corporate fraud control and prevention in modern organisations.

The related empirical studies dwelt on many aspects of fraud control and prevention in commercial banks. For instance, much literature was found on the adequacy of internal control and the role of management in fraud control and prevention. Unfortunately, not much literature was found in the area of availability, the extent of utilization and the effectiveness of corporate fraud control and prevention systems in commercial banks in Enugu state. Not much literature was also found about the problems encountered by the commercial banks in the utilization of corporate fraud control and prevention systems and the strategies for improvement. These gaps are what the present study seeks to fill.

CHAPTER THREE
METHODOLOGY

This chapter describes the procedures used in this study. The procedures include: design of the study, area of the study, population of the study, instrument for data collection, validation of the instrument, reliability of the instrument, administration of the instrument, and method of data analyses.

Design of the Study

The study adopted a descriptive survey design. A survey of the managers, accountants and supervisors of commercial banks in Enugu State was carried out to elicit their opinion on the corporate fraud control and prevention systems in the commercial banks. Survey research design is suitable for this study because survey involves the determination of people's opinion about an existing phenomenon using questionnaire. Survey is also used to justify a current condition or practice and to make better plans for improving the condition. Survey, according to Osuala (2005), focuses on people, the vital facts of people, and their beliefs, opinions, atitudes, motivations and behaviours. Survey for this study was, therefore, used to collect information from the respondents on the corporate fraud control and prevention systems in the commercial banks in Enugu state.

Area of the Study

The area of the study was Enugu State of Nigeria. Enugu State was chosen because as the regional capital of Eastern Nigeria, a reasonable number of commercial banks are operating in the state. 96 commercial bank branches are operating in the state. The commercial banks in the State are also adversely affected by corporate frauds because of the recent use of computers, the

internet and other electronic devices for banking services coupled with huge financial assets handled by the banks. For instance, the commercial banks operating in Enugu state were affected in the 2746 bank frauds that involved about N15 billion reported by Nigeria Deposit Insurance Corporation between 2006 and 2007. Commercial banks in Enugu state were also among the Nigerian commercial banks that lost more than N48 billion to corporate frauds between 2001 and 2006. The list of about 50 failed commercial banks in Nigeria between 1994 and 2006 also included some commercial bank branches that operated in Enugu state. For instance, Cooperative and Commerce Bank Ltd. (CCB) and African Continental Bank Ltd. (ACB), which had their headquarters in Enugu amongst their other branches, went distress mainly because of frauds. Heavy financial losses mainly caused by frauds also made some commercial banks that had some of their branches in Enugu state not to survive the consolidation exercise in the Nigerian banking industry in December 2005. Enugu state was also chosen as the area of the study because the commercial banks operating in the state have many customers spread across business organizations, government ministries, civil servants and other individuals who need protection and services from the banks. The list of the commercial bank branches operating in the state was obtained from the central of Nigeria (CBN).

Population of the Study

The population of the study comprised all the 288 management staff in the 96 commercial bank branches operating in Enugu State. Three management staff from each of the 96 commercial bank branches made up the 288 management staff used for the study. The management staff were the

managers, the accountants and the supervisors of each of the commercial bank branches. These officers were selected because they are the principal staff of the commercial banks and are responsible for the implementation of the fraud control and prevention systems in the commercial banks. They are much more aware of the fraud control and prevention systems utilized in the banks, the extent of the utilization and the effectiveness of the systems than other staff, customers and investors of the banks. Umeh (2004) stated that the management of both the private and public establishment respectively is responsible for the establishment and implementation of the fraud control and prevention systems to achieve the organizational goals. The distribution of the commercial banks and the management staff is shown in table 1. There was no sample in the study. The entire population was studied because the population was manageable.

Table 1:

Population Distribution

S/No	Name of Banks	Number of Branches	Number of Management Staff
1.	Access Bank Plc	2	6
2.	Afribank Plc	5	15
3.	Bank PHB	4	12
4.	Diamond Bank plc	4	12
5.	Ecobank Plc	3	9
6.	Equitorial Trust Bank	2	6
7.	Fidelity Bank Plc	3	9
8.	First Bank of Nigeria Plc	14	42
9.	First City Monument Bank	2	6
10.	First Inland Bank	3	9
11.	Guaranty Trust Bank	3	9
12.	Intercontinental Bank	7	21
13.	Oceanic Bank Plc	6	18
14.	Skye Bank Plc	1	3
15.	Spring Bank Plc	3	9
16.	Stanbic IBTC Bank Plc	1	3
17.	Sterling Bank Plc	1	3
18.	Union Bank of Nigeria Plc	9	27
19.	United bank of Africa	16	48
20.	Wema Bank Plc	1	3
21	Zenith Bank Plc	6	18
Total		**96**	**288**

Source: Central Bank of Nigeria (CBN), October 2008.

Instrument for Data Collection

Structured questionnaire for determining the corporate fraud control and prevention systems in commercial banks was used for gathering data for this study. The questionnaire was developed by the researcher and it contained 97 items that were divided into nine sections (A-I). Section A of the questionnaire

dealt with general information about the respondents. This section contained four questionnaire items with options and blank spaces that enabled the respondents to tick or fill as appropriate.

Section B dealt with research question one. It contained 12 items that were used to collect data to answer research question one. It was structured on a checklist and was used to elicit information from the respondents on the corporate fraud control systems available in commercial banks in Enugu state. The response options "Available" and ''not available" were used.

Section C dealt with research question two. It contained 12 items. This section was used to ascertain the corporate fraud prevention systems available in commercial banks in Enugu state. It was structured on a checklist. The response options were "Available" and "Not Available".

Section D dealt with research question three and it contained 12 items. This section was used to ascertain the opinion of the respondents on the extent of utilization of the corporate fraud control systems in the commercial banks. It was structured on a five–point Likert rating scale and was used to elicit the required information. The response categories were "Always", "Most Times", "Often", "Sometimes" and "seldom".

Section E dealt with research question four. It contained 12 items and was used to ascertain the opinion of the respondents on the extent of utilization of the corporate fraud prevention systems in the commercial banks. It was also structured on a five–point Likert rating scale. The response categories were "Always", "Most Times", "Often", sometimes" and "seldom".

Section F dealt with research question five and it contained 12 items. It was used to ascertain the opinion of the respondents on the effectiveness of the

corporate fraud control systems utilized in the commercial banks. It was structured on a five–point Likert rating scale. The response categories used were “Very effective”, “Effective”, “Rarely Effective”, “Ineffective” and “Very Ineffective”.

Section G dealt with research question six. It contained 12 items and was used to ascertain the opinion of the respondents on the effectiveness of the corporate fraud prevention systems utilized in the commercial banks. It was also structured on a five-point Likert rating scale. The response categories used were “Very Effective”, “Effective”, “Rarely Effective”, “Ineffective” and “Very Ineffective”.

Section H dealt with research question seven. It contained 13 items and was used to ascertain the opinion of the respondents on the problems encountered by the commercial banks in the utilization of the corporate fraud control and prevention systems. The items were also structured on a five–point Likert rating scale and had “Strongly Agree”, “Agree”, “Slightly Agree”, “Disagree” and “Strongly Disagree” as the response options.

Section I dealt with research question eight. This section contained 12 items and was used to ascertain the opinion of the respondents on strategies for enhancing the effective utilization of the corporate fraud control and prevention systems in the commercial banks. The questionnaire items were structured on a five–point Likert rating scale. The response options were “Strongly Agree”, “Agree”, “Slightly Agree”, “Disagree” and “Strongly “Disagree”

Validation of the Instrument

Three specialists from the Department of Vocational Teacher Education University of Nigeria, Nsukka and two professional Accountants in the service

of University of Nigeria, Nsukka subjected the questionnaire to face validation. The researcher requested them to check the clarity, relevance and spelling of the items in the questionnaire. They were also expected to make comments and corrections where necessary. The specialists from the Department of Vocational Teacher Education, UNN ensured the adequacy and the correctness of the contents of the questionnaire while the professional accountants ensured the correctness of the accounting-related items in the questionnaire. They made useful suggestions for the structure and contents of the questionnaire. Their suggestions and observations were used to refine the questionnaire both in structure and contents.

Reliability of the Instrument

Kuder-Richardson [K-R20] reliability test was used to determine the internal consistency of questionnaire items in sections B and C. Cronbcach Alpha Reliability test was used to determine the internal consistency of the items in sections D to I of the questionnaire. The instrument was pre-tested on 30 respondents made up of 10 managers, 10 accountants and 10 supervisors selected from 10 commercial banks in Ebonyi state. This was to ensure that the subjects used in the reliability test were excluded from the study sample. Their responses were used to determine the reliability coefficient for each of the eight clusters of items of the questionnaire. High reliability coefficients of 0.96, 0.98, 0.99, 0.98, 0.98, 0.99, 0.99 and 0.98 were obtained for each of the eight clusters of items in the questionnaire.

Administration of the Instrument

Copies of the questionnaire were personally administered to the respondents by the researcher with the assistance of two trained research

assistants. The researcher trained the research assistants on the duty they were expected to perform. The contents of the questionnaire in addition to the purpose of the study were explained to them to enable them explain same to the respondents as the need arises. They were also informed on how to approach the respondents for easy acceptance, completion and return of the questionnaire. For instance, they should be polite and humble to the respondents and other staff of the banks in the course of the administration and retrieval of the questionnaire. The research assistants were given the list of the commercial bank branches and their locations in Enugu State. The area each research assistant covered was made known to him by the researcher. One research assistant covered Enugu East senatorial zone while another researcher assistant covered Enugu West senatorial zone. The researcher personally covered Enugu North senatorial zone.

Apart from the delivery of the questionnaire to the respondents, the research assistants also assisted the researcher to collect the questionnaire from the respondents. Each of the research assistants covered the same area he covered during the administration of the questionnaire. This reduced the delays associated with completion and returning of questionnaire by respondents. **288** copies of the questionnaire were administered. However, **257** correctly completed copies or **89** percent of the questionnaire was returned and analysed.

Method of Data Analyses

Research questions one and two were analysed using frequencies and percentages while research questions three to eight were analysed using the mean and standard deviation. Values were assigned to the Likert rating scale as follows:

	Response Categories	Point	Boundary Limits
A	Always/Very Effective/Strongly Agree	5	4.50 - 5.00
B	Most Times/Effective/Agree	4	3.50 – 4.49
C	Often/Rarely Effective/Slightly Agree	3	2.50 – 3.49
D	Sometimes/Ineffective/Disagree	2	1.50 – 2.49
E	Seldom/Very Ineffective/Strongly Disagree	1	0.50 – 1.49

The percentage of responses to each item in research questions one and two were computed and interpreted. Items with 50percent and above were taken as "Available" while items with less than 50 percent score were taken as "Not Available". The mean score and the standard deviation of each questionnaire item in research questions three to eight were also computed and interpreted. Standard deviation (SD) was used because it is a measure of dispersion or variability from the mean. Large standard deviation shows that the scores are widely scattered above and below the mean while small standard deviation shows that the scores are tightly clustered around the mean. Uzoagulu (1998) stated that if the standard deviation is large the agreement among the respondents on an issue is loose but if the standard deviation is small there is indication that greater number of people agreed on the issue, case discussed or studied. For instance, he stated that a standard deviation of 0.19 is small while a standard deviation of 1.29 is large. $HO_{1,}$ HO_2, HO_3, HO_4, and HO_5 were tested using t-test statistic at 0.05 level of significance. If the level of significance set by computer was equal to or greater than the level of significance chosen by the researcher, the null hypothesis was accepted. Conversely, if the level of significance set by computer was less than the level of significance chosen by the researcher, the null hypothesis was rejected.

Statistical Package for the Social Sciences (SPSS) was used to analyse the data collected for the study.

CHAPTER FOUR
PRESENTATION AND ANALYSIS OF DATA

In this chapter, the data collected for answering the research questions and testing the hypotheses in the study are presented and analyzed using appropriate tools.

Research Question 1

What are the corporate fraud control systems available in commercial banks in Enugu State?

Research question one was answered using items 1 to 12 of the questionnaire. The responses to the items were analysed and presented in Table 2.

Table 2:
Mean Responses of Respondents on Corporate Fraud Control Systems Available in Commercial Banks

S/No	Items	Available		Not available	
		Frequency	%	Frequency	%
1.	Written operation procedure manual	213	83	44	17
2.	Written procedure for regular credit evaluation, supervision and monitoring	230	89	27	11
3.	Internal and external auditing systems	193	75	64	25
4.	Documented employment-screening procedure	221	86	36	14
5.	Standard system for monitoring employee characteristics and spending patterns	164	64	93	36
6.	Standard system for fraud education and awareness campaigns	208	81	49	19
7.	Standard system for reward and punishment of employees	214	83	43	17
8.	Proper career development programmes for employees	196	76	61	24
9.	Suitable internal control systems	225	88	32	12
10.	Procedures for regular evaluation of fraud risks and opportunities	187	73	70	27
11.	Proper method of posting, placement and disengagement of staff	223	87	34	13
12.	Provision for regular review and update of processes and structures	206	80	51	20

The data presented in Table 2 shows the availability of the corporate fraud control systems in the commercial banks. The result shows that a greater proportion of the respondents indicated that all the corporate fraud control systems listed in the Table were available in the commercial banks. Less than 50 percent of the respondents in each case indicated that the corporate fraud control systems were not available in the commercial banks. The implication of the above findings was that some of the corporate fraud control systems listed in Table 2 were available in the commercial banks. The above findings also implied that the corporate fraud control systems were not adequately available in the commercial banks.

Research Question 2

What are the corporate fraud prevention systems available in commercial banks in Enugu State?

The above research question was answered using items 13-14. The responses to the items were analysed and presented in table 3.

Table 3:
Mean Responses of Respondents on Corporate Fraud Prevention Systems Available in Commercial Banks

S/No	Items	Available		Not Available	
		Frequency	%	Frequency	%
13.	Electronic method of authentication	235	91	22	9
14.	Firewall and data encryption technology	98	38	159	62
15.	Database of lost cheques and other banking instruments	194	75	63	25
16.	Credit and debit alert systems	238	93	19	7
17.	Biometric identifiers for identifying customers	86	33	171	67
18.	Web geolocation technology for locating Internet users	77	30	180	70
19.	Computerized system for monitory bank transactions	217	84	40	16
20.	Overt and closed-circuit surveillance systems	83	32	174	68
21.	Password technology, challenge response and call-back protocols	228	89	29	11
22.	Computer and accounting forensic systems	198	77	59	23
23.	Inter and intra banks connectivity system	237	92	20	8
24.	Database of fraudsters and suspect customers	89	35	168	65

The data presented in Table 3 shows the availability of the corporate fraud prevention systems in the commercial banks. The result shows that a greater proportion of the respondents indicated that the corporate fraud prevention systems listed in items 13, 15, 16, 19, 21, 22 and 23 were available in the commercial banks while less than 50 percent of the respondents indicated that they were not available in the banks. A greater proportion of the

respondents indicated that the corporate fraud prevention systems in items 14, 17, 18, 20 and 24 were not available in the commercial banks while less than 50 percent of the respondents indicated that those items were available in the commercial banks. The implication of the findings in Table 3 was that only seven items in that Table were available in the banks while five items were not available. This also implied that corporate fraud prevention systems were not adequately available in the commercial banks.

Research Question 3

To what extent are the corporate fraud control systems utilized in the commercial banks?

The above research question was answered using items 25 to 36 of the questionnaire. The responses to the items were analysed and presented in Table 4.

Table 4:
Mean Responses of Respondents on the Extent of Utilization of Corporate Fraud Control Systems in Commercial Banks.

S/No	Items	A	MT	O	ST	S	MEAN	Standard Deviation	Remarks
25.	Written operation procedure manual	72	106	33	42	4	3.74	1.09	Most Times
26.	Written procedure for regular credit evaluation,	82	98	53	20	4	3.91	0.99	Most times
27.	Internal and external auditing systems	110	62	56	29	-	3.98	1.05	Most times
28.	Documented employment screening system	93	65	60	39	-	3.83	1.08	Most times
29.	Standard system for monitoring employee characteristics and spending patterns	62	32	27	101	35	2.94	1.43	Often
30.	Standard system for fraud education and awareness campaigns	54	86	41	35	41	3.30	1.37	Often
31.	Standard systems for reward and punishment of employees	83	104	70	-	-	4.05	0.77	Most times
32	Proper career development programmes for employees	123	74	36	24	-	4.15	0.99	Most time
33.	Suitable internal control system	79	97	78	3	-	3.98	0.81	Most times
34.	Procedures for regular evaluation of fraud risks and opportunities	33	40	33	114	47	2.64	1.30	Often
35.	Proper method of posting, placement and disengagement of staff	56	63	88	50	-	3.49	1.04	Often
36.	Provision for regular review and update of processes and structures	71	90	27	23	46	3.46	1.44	Often
	Overall						3.62	1.05	Most times

The data presented in Table 4 shows the extent of utilization of the corporate fraud control systems in the commercial banks. The result shows that items 25 to 28 and items 31 to 33 had mean responses ranging from 3.74 to

4.15, which were within the boundary limit of 3.50-4.49 showing that those items were utilized most times in the commercial banks. The mean responses of items 29, 30, 34, 35 and 36 range from 2.64 to 3.49 and were within the boundary limit of 2.50-3.49 showing that those items were utilized often. The standard deviation of items 25, 27, 28, 30, 34, 35 and 36 which range from 1.04 to 1.44 showed that the opinions of the respondents on those items were not close to one another. This indicated that all the respondents did not have similar opinions on the extent of utilization of those items in the commercial banks. All the items in Table 4 had an average mean of 3.62 and standard deviation of 1.05. The overall mean of 3.62 indicated that all the corporate fraud control systems listed in table 4 were utilized most times in the commercial banks. However, the average standard deviation of 1.05 indicated that all the respondents did not have similar opinion on the extent of utilization of those systems in the commercial banks. Since none of the corporate fraud control systems was utilized always in the banks it implied that the corporate fraud control systems were not extensively utilized in the commercial banks.

Research Question 4

To what extent are the corporate fraud prevention systems utilized in the commercial banks?

The above research question was answered using items 37 to 48 of the questionnaire. The responses to the items were analysed and presented in Table 5.

Table 5:
Mean Responses of Respondents on the Extent of Utilization of Corporate Fraud Prevention Systems in Commercial Banks

	Items	A	MT	O	ST	S	Mean	Standard Deviation	Remarks
37	Electronic method of authentication and authorization of payments	122	66	41	28	-	4.10	1.03	Most times
38	Firewall and data encryption technology	76	83	58	37	3	3.75	1.07	Most times
39	Database of lost cheques and other banking instruments	81	111	31	29	5	3.91	1.03	Most times
40	Credit and debit alert system	79	107	53	18	-	3.96	0.89	Most times
41	Biometric identifiers for identifying customers	26	33	92	88	18	2.85	1.07	Often
42	Web geolocation technology for locating internet users	34	17	85	113	8	2.83	1.07	Often
43	Computerized system for monitoring bank transactions	62	98	51	46	-	3.68	1.03	Most times
44	Overt and closed- circuit surveillance systems	37	70	121	29	-	3.45	0.87	Often
45	Password technology, challenge-response and call-back protocols	83	104	36	34	-	3.92	O.99	Most times
46	Computer and accounting forensic systems	26	91	78	39	23	3.23	1.11	Often
47	Inter and intra banks connectivity systems	87	95	35	29	11	3.85	1.14	Most times
48	Database of fraudsters and suspected customers	51	13	122	71	-	3.17	1.05	Often
	Overall						3.56	0.96	Most times

Always (A), often {o), Most times (MT), sometimes (ST), Seldom (S)

The data presented in Table 5 shows the extent of utilization of the corporate fraud prevention systems in the commercial banks. The data presented in Table 5 also shows that the mean responses of the respondents

indicated that the corporate fraud prevention systems listed in items 37, 38, 39,40,43,45 and47 were utilized most times in the commercial banks. Only the corporate fraud prevention systems in items 41, 42, 44 and 46 were utilized often in the commercial banks. The mean responses of the respondents showed that none of the corporate fraud prevention systems in Table 5 was utilized always, sometimes or seldom in the commercial banks. Although the average mean responses of 3.56 showed that all the items were utilized most times in the banks, it can be seen from Table 5 that corporate fraud prevention systems were not always or extensively utilized in the commercial banks. The average standard deviation of all the items in Table 5 which was 0.96 indicated that all the respondents similarly agreed that the corporate fraud prevention systems were utilized most times but not always.

Research Question 5

How effective are the corporate fraud control systems in controlling frauds in the commercial banks?

The above research question was answered using items 49 to 60 of the questionnaire. The responses to the items were analysed and presented in Table 6.

Table 6:
Mean Responses of Respondents on the Effectiveness of the Corporate Fraud Control Systems in Controlling Frauds in Commercial Banks

	Items	VE	E	RE	I	VI	Mean	Standard Deviation	Remarks
49	Written operation procedure manual	88	123	36	8	2	4.12	0.82	Effective
50.	Written procedure for regular credit evaluation, supervision and monitoring	103	76	58	17	3	4.01	0.10	Effective
51.	Internal and external auditing systems	74	119	43	21	-	3.96	0.89	Effective
52.	Documented employment screening procedure	53	85	98	17	4	3.65	0.93	Effective
53.	Standard system for monitoring employee characteristics and spending patterns	23	31	118	61	24	2.88	1.04	Rarely effective
54.	Standard system of fraud education and awareness campaigns	81	142	28	6	-	4.16	0.70	Effective
55.	Standard system for reward and punishment of employees	153	76	22	6	-	4.46	0.75	Effective
56.	Proper career development programmes for employees	59	136	28	16	18	3.79	1.08	Effective
57.	Suitable internal control systems	63	138	37	15	4	3.94	0.87	Effective
58.	Procedure for regular evaluation of fraud risks and opportunities	116	82	41	16	2	4.14	0.96	Effective
59.	Proper method of posting, placement and disengagement of staff	77	64	106	8	2	3.80	0.93	Effective
60.	Provision for regular review and update of processes and structures	138	81	33	2	3	4.36	0.82	Effective
*	Overall						3.94	0.83	Effective

Very effective (VE), effective (E), rarely effective (RE), ineffective (I), very ineffective (VI)

The data presented in Table 6 shows the extent of the effectiveness of the corporate fraud prevention systems in the commercial banks. As can be seen from Table 6, the mean responses of the respondents show that the corporate fraud control systems listed in all the items in the Table were

effective in controlling corporate frauds in the banks except standard system for monitoring employee characteristics and their spending patterns which was listed as item 53. The respondents indicated that item 53 is rarely effective in fraud control in the commercial banks. The respondents' average mean responses of 3.94 showed that all the corporate fraud control systems were effective in controlling fraudulent activities in the banks while the average standard deviation of 0.83 showed that most of the respondents were of similar opinion that the corporate fraud control systems were effective in the commercial banks. The findings in Table 6 showed that none of the corporate fraud control systems was very effective in fraud control in the banks.

Research Question 6

How effective are the corporate fraud prevention systems in preventing frauds in the commercial banks?

The above research question was answered using items 61 to 72 of the questionnaire. The responses to the items were analysed and presented in Table 7.

Table 7:
Mean Responses of Respondents on the Effectiveness of Corporate Fraud Prevention Systems in Preventing Frauds in Commercial Banks.

	Items	VE	E	RE	I	VI	Mean	Standard Deviation	Remarks
61.	Electronic method of authentication and authorization of payments	118	85	36	12	6	4.16	0.99	Effective
62.	Firewall and data encryption technology	132	74	41	7	3	4.26	0.91	Effective
63.	Database of lost cheques and other banking instruments	126	91	27	13	-	4.28	0.85	Effective
64.	Credit and debt alert systems	84	112	46	9	6	4.01	0.93	Effective
65.	Biometric identifiers for identifying customers	49	158	31	11	8	3.89	0.87	Effective
66.	Web geolocation technology for locating internet users	82	128	23	21	3	4.03	0.92	Effective
67.	Computerized system for monitoring bank transactions	93	101	46	17	-	4.05	0.90	Effective
68.	Overt and closed circuit surveillance system	114	87	42	5	9	4.14	0.99	Effective
69.	Password technology, challenge–response and call-back protocols	46	121	68	18	4	3.73	0.89	Effective
70.	Computer and accounting forensic systems	83	129	34	4	7	4.08	0.87	Effective
71.	Inter and intra banks connectivity system	108	67	48	34	-	3.97	1.07	Effective
72.	Database of fraudsters and suspected customers	78	139	36	4	-	4.13	0.70	Effective
	Overall						4.06	0.85	Effective

Very Effective (VE), Effective (E), Rarely Effective (RE), Ineffective (I), Very Ineffective (VI).

The data presented in Table 7 shows the extent of the effectiveness of the corporate fraud prevention systems in the commercial banks. The mean responses of the respondents in Table 7 show that all the corporate fraud prevention systems listed in the Table were effective in preventing fraudulent activities in the commercial banks. The average mean responses of 4.06 in the

Table also indicated that all the corporate fraud prevention systems were effective in fraud prevention in the banks. The average standard deviation of 0.85 in the Table as well showed that most of the respondents were of the opinion that the corporate fraud prevention systems were effective in preventing fraudulent activities in the commercial banks. As can be seen from Table 7, the mean responses of the respondents indicated that none of the corporate fraud prevention systems was very effective in the prevention of corporate frauds in the commercial banks.

Research Question 7

What are the problems encountered by the commercial banks in the utilization of the corporate fraud control and prevention systems?

Research question 7 was answered using items 73 to 85 of the questionnaire. The responses to the items were analysed and presented in Table 8.

Table 8:
Mean Responses of Respondents on the Problems Encountered by Commercial Banks in the Utilization of Corporate Fraud Control and Prevention Systems

	Items	SA	A	Sa	D	SD	Mean	Standard Deviation	Remarks
73	The cost of acquiring and implementing the anti-fraud systems is very high	58	133	42	24	-	3.88	0.87	Agree
74	The cost of training personnel to operate the anti-fraud systems is very high	69	118	57	9	4	3.93	0.88	Agree
75.	Proper implementation of the systems is limited by collaboration of bank officials, staff and third parties to commit fraud	51	136	32	27	11	3.74	1.03	Agree
76.	Heavy work load leads to errors that limit proper implementation of the systems	54	88	94	21	-	3.68	0.90	Agree
77.	Many of the systems operators are not competent	58	73	106	13	7	3.63	0.98	Agree
78.	Instability in power supply affects the successful implementation of the systems	76	144	33	4	-	4.14	0.69	Agree
79.	The large volume of data to be stored and retrieved poses a problem to proper utilization of the system	47	38	151	15	6	3.41	0.93	Slightly Agree
80.	The complexity and sophistication in the systems limit successful utilization of the systems	71	125	44	13	4	3.96	0.89	Agree
81.	Successful implementation of the systems is limited by management over-ride of internal controls	19	27	108	87	16	2.79	0.97	Slightly Agree
82.	Unprofessional and unethical behaviours exhibited by both management and staff sometimes limit successful utilization of the systems	30	14	139	71	3	2.99	0.92	Slightly Agree
83.	Customers and employees poor perception of the systems affects the successful implementation of the systems	66	112	52	22	5	3.82	0.97	Agree
84.	Too many anti-fraud systems make the implementation unwieldy	18	37	143	59	-	3.05	0.81	Slightly Agree
85.	Unclearly defined aspects of the banks organizational structure cause unnecessary delays in the implementation of the systems	64	139	48	4	2	4.01	0.76	Agree
*	Overall						3.62	0.83	Agree

Strongly Agree (SA), Agree (A), Slightly Agree (Sa), Disagree (D), strongly disagree (SD)

The data presented in Table 8 shows the respondents' level of agreement on the problems encountered by the commercial banks in the utilization of the corporate fraud control and prevention systems. As can be seen from the data presented in Table 8, items 73 to 78, items 80, 83 and 85 had mean scores ranging from 3.63 to 4.14 which were within the boundary limit of 3.50-4.49. It implied that the respondents agreed that those items were problems encountered by the commercial banks in the utilization of the corporate fraud control and prevention systems. Items 79, 81, 82, and 84 had mean scores ranging from 2.79 to 3.41 which were within the boundary limit of 2.50-3.49 which implied that the respondents slightly agreed that those items were problems encountered by the commercial banks in the utilization of the corporate fraud control and prevention systems. None of the respondents had strong agreement, disagreement or strong disagreement on any of the items as a problem encountered in the utilization of the corporate fraud control and prevention systems.

As can also be seen from table 8, items 73, 74 and 76 to 85 had low standard deviation ranging from 0.69 to 0.98. It then implied that more of the respondents were close in their level of agreement to those items as problems encountered by the commercial banks in the utilization of the corporate fraud control and prevention systems. Only item 75 had a high standard deviation of 1.03, which implied that more of the respondents were not close in their level of agreement to that item as a problem encountered by the commercial banks in the utilization of the corporate fraud control and prevention systems.

The average mean to all the items in Table 8 was 3.62, which implied that the respondents agreed that all the items were problems encountered by the commercial banks in the utilization of the corporate fraud control and prevention systems. The entire items in table 8 had an average standard deviation of 0.83 which implied that more of the respondents, all taken together for the entire items, were close in their level of agreement to all the items as problems encountered by the commercial banks in the utilization of the corporate fraud control and preventions systems.

Research Question 8

What are the strategies for enhancing the effective utilization of the corporate fraud control and prevention systems in the commercial banks?

Research question 8 was answered using items 86 to 97 of the questionnaire. The responses to the items were analysed and presented in Table 9.

Table 9:
Mean Responses of Respondents on the Strategies for Enhancing the Effective Utilization of the Corporate Fraud Control and Prevention Systems in the Commercial Banks.

S/N	Items	SA	A	Sa	D	SD	Mean	Standard Deviation	Remarks
86	Enough funds should always be set aside in the banks budget for the installation and implementation of fraud control and prevention systems	144	68	37	5	3	4.34	0.88	Agree
87	Specialized training, seminars and workshops should be regularly organized for both staff and management.	152	71	34	__	__	4.46	0.72	Agree
88	More competent operators for the fraud control and prevention systems should be employed to reduce workload.	43	138	74	2	__	3.86	0.69	Agree
89	Greater regulatory oversight is needed to check the excesses of both staff and management.	46	162	44	3	2	3.96	0.68	Agree
90	Sustainable programmes for continuous education and awareness of all bank stakeholders in fraud control and prevention should be maintained.	81	132	26	11	7	4.03	0.91	Agree
91	The organizational structure of the bank should be clearly defined and monitored to check manipulation by both management and staff.	73	119	65	__	__	4.03	0.73	Agree
92	Single systems that can be used for many operations in fraud control and prevention should be used to reduce costs.	24	62	148	17	6	3.32	0.82	Slightly Agree
93.	The fraud control and prevention systems should be regularly reviewed and updated to match with emerging technologies	79	123	46	7	2	4.05	0.86	Agree
94.	Adequate effort should be given to research and development in fraud control and prevention	149	63	39	8	-	4.37	0.85	Agree
95.	Adequate and commensurate incentives should be given to system operators and other employees	162	74	21	-	-	4.55	0.64	Slightly Agree
96.	An automatic alternative source of power supply should be installed to alleviate the problem of frequent power failure	81	126	44	6	-	4.10	0.76	Agree
97.	The acquisition and implementation of the anti-fraud systems should be made tax – free by government	42	113	98	4	-	3.75	0.74	Agree
*	Overall						4.07	0.70	Agree

Strongly agree (SA), Agree (A), Slightly agree (Sa), Disagree (D), strongly disagree (SD).

The data presented in Table 9 shows the respondents level of agreement on the strategies needed by the commercial banks for enhancing the effective utilization of the corporate fraud control and prevention systems. The data presented in table 9 shows that all the items listed except items 92 and 95 had mean scores ranging from 3.75 to 4.37. This implied that the respondents agreed that all the strategies stated in those items could enhance the effective utilization of the corporate fraud control and prevention systems in the commercial banks. Item 92 had a mean score of 3.32 implying that the respondents slightly agreed that single systems that can be used for many operations in fraud control and prevention should be used to reduce costs to enhance the effective utilization of corporate fraud control and prevention systems. Item 95 had a mean score of 4.55, which implied that the respondents strongly agreed that the strategy stated in the item could enhance the effective utilization of the corporate fraud control and prevention systems in the commercial banks. Each of the items in the above Table had low standard deviation ranging from 0.04 to 0.91 which implied that most of the respondents were close in their level of agreement on each strategy for enhancing the effective utilization of the corporate fraud control and prevention systems in the commercial banks.

The average mean score for all the items in Table 9 was 4.07 which implied that the respondents agreed that all the strategies listed in that Table could enhance the effective utilization of the corporate fraud control and prevention systems in the commercial banks. The average standard deviation for all the items in Table 9 was 0.70. This low standard deviation implied that most of the respondents were close in agreement that all the strategies could enhance the effective utilization of the corporate fraud control and prevention systems in the commercial banks.

Hypothesis one

There is no significant difference in the mean responses of the management staff in new and old generation banks on the extent of utilization of the corporate fraud control and prevention systems in the commercial banks.

After testing the null hypothesis above with t-test statistic at 0.05 level of significance, the results obtained were as presented in items 25 to 36 in Table 10.

Table 10:

Summary of T-test Statistic of Mean Responses of Management Staff in Old and New Generation Banks on the Extent of Utilization of the Corporate Fraud Control Systems in the Commercial Banks.

S/N	Items	New generation banks N= 134		Old generation banks $N_{=123}$		t-value	Sig. 2--tailed	Decision
		X	SD	X	SD			
25.	Written operation procedure manual	3.54	1.04	3.95	1.11	3.09	0.00	Significant
26.	Written procedure for regular credit evaluation, supervision and monitoring	4.07	0.94	3.74	1.01	2.69	0.01	Significant
27.	Internal and external auditing systems	3.87	1.12	4.11	0.95	-1.90	0.06	Not Significant
28.	Documented employment screening procedure	3.89	1.05	3.77	1.11	0.86	0.39	Not Significant
29.	Standard system for monitoring employee characteristics and spending patterns	2.98	1.37	2.90	1.48	0.42	0.67	Not Significant
30.	Standard system for fraud education and awareness campaigns	3.02	1.47	3.60	1.17	-3.47	0.00	Significant
31.	Standard system for reward and punishment of employees	4.04	0.79	4.07	0.75	-0.29	0.77	Not Significant
32.	Proper career development programmes for employees	4.21	0.89	4.09	1.08	0.97	0.33	Not Significant
33.	Suitable internal control system	3.89	0.85	4.08	0.76	-1.92	0.06	Not Significant
34.	Procedure for regular evaluation of fraud risks and opportunities	2.69	1.31	2.59	1.29	0.57	0.57	Not Significant
35.	Proper method of posting, placement and disengagement of staff	3.41	0.99	3.57	1.09	-1.22	0.22	Not Significant
36.	Provision for regular review and update of processes and structures	3.65	1.33	3.24	1.52	2.28	0.02	Significant
*	Overall	3.60	1.04	3.64	1.06	-0.31	0.76	Not Significant

* $df = N_1 + N_2 - 2 = 123 + 134\text{-}2 = 255$

The t-test analysis in table 10 showed that the levels of significance set by computer for the t-values for items 25, 26 30 and 36 were lower than 0.05 level of significance chosen by the researcher for testing the hypothesis. It, therefore, implied that there existed significant difference in the mean responses of management staff in new and old generation banks on the extent of utilization of each of those items in the commercial banks. The null hypothesis was, therefore, rejected in each of those cases.

The level of significance set by computers for items 27, 28, 29, 31, 32, 33, 34 and 35 was greater than 0.05 level of significance chosen by the researcher to test the above hypothesis ($\mathbf{HO_1}$). It implied that there existed no significant difference in the mean responses of respondents in new and old generation banks on the extent of utilization of the corporate fraud control systems listed in those items. The null hypothesis in each of those items was, therefore, accepted. The overall level of significance set by computer for the overall calculated t–value for all the items in Table 10 was greater than 0.05 level of significance chosen by the researcher for testing the null hypothesis ($\mathbf{HO_1}$). It implied that there was no significant difference in the mean responses of respondents in new and old generation banks on the extent of utilization of the corporate fraud control systems in the commercial banks. The above findings implied that both the respondents from new and old generation banks had similar responses on the extent of utilization of the corporate fraud control systems in the commercial banks. The null hypothesis ($\mathbf{HO_1}$) was, therefore, accepted.

Hypothesis Two

There is no significant difference in the mean responses of management staff in new and old generation banks on the extent of utilization of the corporate fraud prevention systems in the commercial banks.

The results obtained after testing the above null hypothesis with t-test statistic at 0.05 level of significance were as presented in items 37 to 48 in Table 11.

Table 11:

Summary of T-test Statistic of Mean Reponses of Management Staff in New and Old Generation Banks on the Extent of Utilization of the Corporate Fraud Prevention Systems in the Commercial Banks.

S/No	Items	New generation banks $N_{=134}$		Old generation Banks N=123		t-Value	Sig. 2–tailed	Decision
		X	SD	X	SD			
37.	Electronic method of authentication and authorization of payments	4.13	0.99	4.06	1.08	0.60	0.55	Not Significant
38.	Firewall and data encryption technology	3.85	1.04	3.63	1.10	1.63	0.11	Not Significant
39.	Database of lost cheques and other banking instruments	3.96	0.90	3.85	1.16	0.85	0.40	Not significant
40.	Credit and debit alert system	4.03	0.89	3.89	0.89	1.29	0.20	Not Significant
41.	Biometric identifiers for identifying customers	2.90	1.07	2.80	1.06	0.74	0.46	Not Significant
42.	Web geolocation technology for locating internet users	2.81	1.08	2.85	1.06	-0.24	0.81	Not Significant
43.	Computerized system for monitoring bank transactions	3.59	1.10	3.79	0.94	-1.55	0.12	Not Significant
44.	Overt and closed-circuit surveillance system	3.46	0.86	3.43	0.89	0.29	0.77	Not Significant
45.	Password technology, challenge-response and call-back protocols	4.07	0.83	3.76	1.13	2.53	0.01	Significant
46.	Computer and accounting forensic systems	3.32	1.02	3.12	1.19	1.44	0.15	Not Significant
47.	Inter and intra banks connectivity systems	3.86	1.15	3.84	1.13	0.15	0.88	Not Significant
48.	Database of fraudsters and suspected customers	3.01	0.99	3.35	1.08	-2.65	0.01	Significant
*	Overall	3.58	0.93	3.53	0.99	0.44	0.66	Not Significant

* $df = N_1 + N_2 - 2 = 134 + 123 - 2 = 255$

The t-test analysis in Table 11 showed that the level of significance set by computer for the calculated t–value for each of the items listed except items 45 and 48 was greater than 0.05 level of significance chosen by the researcher for testing the hypothesis. This implied that there was no significant difference in the mean responses of respondents in new and old generation banks on the extent of utilization of those corporate fraud prevention systems in the commercial banks. The null hypothesis as regards those items was, therefore, accepted. The levels of significance set by computer for the t-values in items 45 and 48 in Table 11 were lower than 0.05 level of significance chosen by the researcher for testing the null hypothesis. This implied that there was significant difference in the mean responses of the respondents in both the new and old generation banks. The null hypothesis as it regards those items was, therefore, rejected. The level of significance set by computer for the overall calculated t-value for all the items in the Table 11 was greater than 0.05 level of significance chosen by the researcher for testing the null hypothesis ($\mathbf{HO_2}$). It implied that there was no significant difference in the mean responses of the respondents in new and old generation banks on the extent of utilization of the corporate fraud prevention systems in the commercial banks. The findings in Table 11 implied that both the respondents from new and old generation banks had similar opinions on the extent of utilization of the corporate fraud prevention systems in the commercial banks. The null hypothesis ($\mathbf{HO_2}$) was, therefore, generally accepted.

Hypothesis Three

There is no significant difference in the mean responses of management staff in new and old generation banks on the effectiveness of the corporate fraud control systems in controlling frauds in the commercial banks.

The results obtained after testing the above hypothesis with t–test statistic at 0.05 level of significance were as presented in items 47 to 60 in table 12.

Table 12:

Summary of T-test Statistic of Mean Responses of Management Staff in New and Old Generation Banks on the Effectiveness of the Corporate Fraud Control Systems in the Commercial Banks.

S/No	ITEMS	New generation banks N = 134		Old generation banks N =123		t- value	Sig. 2-tailed	Decision
		$\bar{X}$	SD	$\bar{X}$	SD			
49.	Written operation procedure manual	3.96	0.84	4.28	0.76	-3.22	0.00	Significant
50.	Written procedure for regular credit evaluation, supervision and monitoring	3.97	1.05	4.05	0.95	-0.63	0.53	Not Significant
51.	Internal and external auditing systems	4.03	0.84	3.88	0.929	1.38	0.17	Not Significant
52.	Documented employment – screening system	3.57	0.94	3.72	0.92	-1.28	0.20	Not Significant
53.	Standard system for monitoring employee characteristics and spending patterns	2.80	1.05	2.96	1.02	-1.24	0.22	Not Significant
54.	Standard system for fraud education and awareness campaigns	4.18	0.68	4.14	0.73	0.47	0.64	Not Significant
55.	Standard system for reward and punishment of employees	4.44	0.70	4.49	0.80	-0.51	0.61	Not Significant
56.	Proper career development programmes for employees	3.75	1.15	3.83	1.01	-0.61	0.54	Not significant
57.	Suitable internal control systems	3.89	0.94	3.99	0.79	-0.95	0.34	Not significant
58.	Procedures for regular evaluation of fraud risks and opportunities	4.15	0.98	4.14	0.94	0.09	0.93	Not Significant
59.	Proper method of positing, placement and disengagement of staff	3.88	0.93	3.72	0.93	1.42	0.16	Not Significant
60.	Provision for regular review and update of processes and structures	4.37	0.77	4.34	0.88	0.31	0.76	Not significant
*	Overall	3.92	0.84	3.96	0.83	-0.43	0.66	Not Significant

* $df = N_1 + N_2 - 2 = 134 + 123\text{-}2 = 255$

The t–test analysis in table 12 showed that the level of significance set by computer for the t–value to item 49 was lower than 0.05 level of significant set by the researcher for testing the null hypothesis which implied that there was significant difference in the mean responses of respondents in the new and old generation banks on the effectiveness of written operation procedure manual in fraud control in the commercial banks. The null hypothesis as it regards item 49 was therefore rejected. For items 50 to 60, the level of significance set by computer for the calculated t-value in each of those items was greater than 0.05 level of significance set by the researcher for testing the hypothesis. This implied that there was no significant difference in the mean responses of respondents in new and old generation banks on the effectiveness of the corporate fraud control systems listed in those items in fraud control in the commercial banks. The null hypothesis for each of the items, 50 to 60, was accepted.

The overall level of significance of 0.66 set by the computer for the calculated t-value of -0.43 for the entire items in the Table 12 was greater than 0.05 level of significant set by the researcher for testing the null hypothesis (**HO_3**). It implied that there was no significance difference in the mean responses of respondents in new and old generation banks on the effectiveness of the corporate fraud control systems in the commercial banks. It also implied that the respondents from new and old generation banks had similar opinions on all items in table 12. The null hypothesis for all the items in the Table 12 was, therefore, accepted

Hypothesis Four

There is no significant difference in the mean responses of management staff in new and old generation banks on the effectiveness of the corporate fraud prevention systems in preventing frauds in the commercial banks.

The results obtained after testing the above hypothesis with t-test statistic at 0.05 level of significance were as presented in items 61 to 72 in Table 13.

Table 13:

Summary of T-test Statistic of Mean Responses of Management Staff of New and Old Generation Banks on the Effectiveness of the Corporate Fraud Prevention Systems in the Commercial Banks.

S/No	Items	New generation banks. N_1= 134		Old generation banks. $N_{3=}$ 123		t-value	Sig. 2-taled	Decision
		X	SD	X	SD			
61.	Electronic method of authentication and authorization of payments	4.16	0.98	4.15	1.00	0.14	0.89	Not significant
62.	Firewall and data encryption technology	4.10	1.01	4.44	0.75	-3.00	0.00	Significant
63.	Database of lost cheques and other banking instruments	4.27	0.87	4.30	0.83	-0.30	0.76	Not Significant
64.	Credit and debit alert systems	3.98	0.98	4.04	0.86	-0.54	0.59	Not significant
65.	Biometric identifiers for identifying customers	3.81	0.95	3.98	0.76	-1.50	0.14	Not significant
66.	Web geolocation technology for locating internet users.	3.93	0.99	4.14	0.82	-1.80	0.07	Not significant
67.	Computerized system for monitoring bank transactions	4.02	0.91	4.08	0.88	-0.53	0.60	Not significant
68.	Overt and closed circuit surveillance systems	4.14	0.97	4.13	0.02	0.09	0.93	Not significant
69.	Password technology, challenge–response and call–back protocols	3.75	0.8795	3.70	0.9048	0.49	0.625	Not significant
70.	Computer and accounting forensic systems	4.24	0.90	3.90	0.80	3.14	0.00	Significant
71.	Inter and intra banks connectivity system	3.99	1.07	3.94	1.07	0.37	0.71	Not significant
72.	Database of fraudsters and suspected customers	4.12	0.69	4.15	0.71	-0.31	0.76	Not significant
*	Overall	4.04	0.88	4.08	0.81	-0.32	0.75	Not significant

* $df = N_1 + N_2 - 2 = 134 + 123-2 = 25$

The t-test analysis in table 13 showed that the level of significance set by computer for the t-values of each of the items except items 62 and 70 were greater than the level of significance chosen by the researcher. This implied that the t-value in each of those items was not significant which also implied that there was no significant difference in the mean responses of management staff in new and old generation banks on the effectiveness of the corporate fraud prevention systems utilized in the commercial banks. The null hypothesis was, therefore, accepted as it concerned those items. The level of significance set by computer for the t-values of items 62 and 70 respectively were lower than 0.05 level of significance chosen by the researcher for testing the null hypothesis. The t-value in each of the items was therefore significant. The null hypothesis as regards the two items was, therefore, rejected.

The overall level of significance set by computer for all the items in Table 13 was 0.75 which was greater than 0.05 level of significance chosen by the researcher for testing the null hypothesis ($\mathbf{HO_4}$) implying that the overall t-value for all the items was not significant. The null hypothesis was, therefore, accepted considering all the items together. It implied that there was no significant difference between the mean responses of management staff in new and old generation banks on the effectiveness of the corporate fraud prevention systems in the commercial banks. The respondents had similar responses on all the items listed in the above Table. The null hypothesis ($\mathbf{HO_4}$) was, therefore, accepted.

Hypothesis five

There is no significant difference in the mean responses of management staff in new and old generation banks on the problems encountered by commercial banks in the utilization of the corporate fraud control and prevention systems.

The results obtained after testing the above hypothesis with t-test statistic at 0.05 level of significance were as presented in items 73 to 85 in Table 14.

Table 14:
Summary of t-test Statistic of Mean Responses of Management Staff in New and Old Generation Banks on the Problems Encountered by Commercial Banks in the Utilization of the Corporate Fraud Control and Prevention Systems

S/N	Items	New generation Banks N= 134		Old generation Banks N=123		t-Value	Sig. 2-tailed	Decision
		X	SD	X	SD			
73.	The cost of acquiring and implementing the anti-fraud systems is very high	3.84	0.97	3.92	0.74	-0.77	0.45	Not significant
74.	The cost of training personnel to operate the anti-fraud systems is very high	4.02	0.77	3.83	0.97	0.77	0.08	Not significant
75.	Proper implementation of the systems is limited by collaboration of bank officials, staff and third parties to commit fraud.	3.85	0.95	3.61	1.11	1.88	0.06	Not significant
76.	Heavy work load leads to errors that limit proper implementation of the systems	3.15	0.96	3.87	0.78	-3.30	0.00	significant
77.	Many of the systems operators are not competent	3.63	1.05	3.63	0.90	-0.06	0.95	Not significant
78.	Instability in power supply affects the successful implementation of the systems	4.19	0.64	4.08	0.73	1.23	0.22	Not significant
79.	The large volume of data to be stored and retrieved poses a problem to proper utilization of the systems	3.36	0.98	3.46	0.88	-0.90	0.37	Not significant
80.	The complexity and sophistication in the systems limit successful utilization of the systems	3.96	0.80	3.96	0.98	-0.04	0.97	Not significant
81.	Successful implementation of the systems is limited by management over-ride of internal control	2.82	1.02	2.76	0.93	0.53	0.60	Not significant
82.	Unprofessional and unethical behaviour exhibited by both management and staff sometimes limits successful utilization of the systems.	3.01	0.8885	2.97	0.9576	0.35	0.729	Not significant
83.	Customer and employees poor perception of the systems affects the successful implementation of the systems	3.81	0.93	3.85	1.02	-0.33	0.75	Not significant
84.	Too many anti-fraud systems make implementation unwieldy	3.01	0.78	3.10	0.84	-0.82	0.41	Not significant
85.	Unclearly defined aspects of the organizational structure cause unnecessary delays in the implementation of the systems	3.96	0.76	4.06	0.75	-1.00	0.32	Not significant
*	Overall	3.61	0.82	3.62	0.83	-0.10	0.92	Not significant

* $df = N_1+N_2 -2 = 134 + 123-2 = 255$

The t-test analysis in table 14 showed that the level of significance set by computer for the t-values in each of the items except item 76 were greater than 0.05 level of significance chosen by the researcher to test the above hypothesis (**HO_5**). This implied that there was no significant difference in the mean responses of the management staff in new and old generation banks on the problems encountered by commercial banks in the utilization of the corporate fraud control and prevention systems as it regards those items. The hypothesis was accepted for each of items 73 to 85 except items 76. The level of significance set by computer for the t-value for item 76 was lower than 0.05 level of significance chosen by the researcher to test the hypothesis. It implied that the difference in the mean responses of the management staff of new and old generation banks as it regards item 76 was significant. As it regards item 76, the null hypothesis was rejected.

The overall level of significance set by computer for the overall t-value in the Table 14 was greater than 0.05 level of significance chosen by the researcher to test the hypothesis (**HO_5**). It implied that the difference in the mean responses of the management staff in new and old generation banks on the problems encountered by commercial banks in the utilization of the corporate fraud control and prevention systems was not significant. The null hypothesis (**HO_5**) was therefore accepted as it regards all the items in the Table.

Major Findings of the Study

The findings of the study were presented according to the research questions and hypotheses as follows.

Research questions

1. With regard to the corporate fraud control systems available in the commercial banks, it was found that the following corporate fraud control systems were available in most of the commercial banks:

a. written operation procedure manual,

b. internal and external auditing systems,

c. documented employment–screening procedure,

d. proper career development programmes for employees,

e. Suitable internal control systems and

f. procedures for regular evaluation of fraud risks and opportunities.

2. With regard to the availability of the corporate fraud prevention systems in the commercial banks, it was found that the following corporate fraud prevention systems were available in most of the commercial banks:

a. Electronic method of authentication and authorization of payments systems,

b. Credit and debit alert systems,

c. Computerized system of monitoring bank transactions,

d. Password technology, challenge–response and call-back protocols and

e. Computer and accounting forensic systems.

On the other hand, it was found that biometric identifiers, web geolocation technology, firewall and data encryption technology, and database of fraudsters and suspected customers were available only in few of the commercial banks.

3. With regard to the extent of utilization of the corporate fraud control systems in the commercial banks, it was found that

a. Internal and external auditing systems were utilized most times in most of the commercial banks.

b. Suitable internal control system was utilized most times for fraud control in most of the banks.

d. Standard system for reward and punishment of employees was utilized most times to control frauds in the banks.

e. The commercial banks often utilized the system of monitoring employee characteristics and spending patterns.

4. With regard to the extent of utilization of the corporate fraud prevention systems in the commercial banks, it was found that

a. Credit and debit alert systems were most times utilized in most of the banks to prevent account frauds.

b. The banks most times utilized the electronic method of authentication and authorization of payments.

c. The banks often utilized biometric identifiers to identify customers to prevent fraudulent activities.

d. Password technology, challenge–response and call-back protocols were most times utilized in most of the commercial banks to prevent fraudulent activities.

5. With regard to the effectiveness of the corporate fraud control systems in controlling frauds in the commercial banks, it was found that the following systems were effective in controlling fraudulent activities in the banks:

a. Written operation procedure manual,

b. Internal and external auditing systems,

c. Regular review and update of processes and structures,

d. Proper career development programmes for employees and

e. Written procedure for regular credit evaluation, supervision and monitoring.

6. It was found that the following corporate fraud prevention systems were effective in preventing fraudulent activities in the commercial banks:

a. Credit and debit alert systems,

b. Overt and closed–circuit surveillance systems,

c. Password technology, challenge–response and call-back protocols,

d. Electronic method of authentication and authorization of payments and,

e. Biometric identifiers for identifying customers.

7. With regard to the problems encountered by commercial banks in the utilization of the corporate fraud control and prevention systems, it was found that

a. Proper implementation of the systems was limited by collaboration of bank officials, staff and third parties to commit fraud.

b. The complexity and sophistication in the systems limited the successful utilization of the systems because many of the systems operators were not competent.

c. Instability in power supply affected the successful implementation of the corporate fraud control and prevention systems.

d. Customers' and employees' poor perception of the systems affected the successful implementation of the anti-fraud systems.

e. Heavy workload led to errors that limited proper implementation of the systems.

8. With regard to the strategies that should be adopted to enhance the effective utilization of the corporate fraud control and prevention systems in the commercial banks it was found that

a. Specialized training, seminars and workshops should be regularly organized for both staff and management.

b. More competent operators for the fraud control and prevention systems should be employed to reduce workload and errors that could arise from it.

c. Sustainable programmes for continuous education and awareness of all bank stakeholders in fraud control and prevention should be maintained.

d. The fraud control and prevention systems should be regularly reviewed and updated to match with emerging technologies.

e. Adequate and commensurate incentives should be given to systems operators and other employees for effective utilization of the corporate fraud control and prevention systems in the commercial banks.

Hypotheses

HO_1: The findings pertaining to this hypothesis revealed that there was no significant difference in the mean responses of the management staff from new and old generation banks on the extent of utilization of the following corporate fraud control systems in the commercial banks:

a. Internal and external auditing systems,

b. Standard system for reward and punishment of employees,

c. Suitable internal control system,

d. Documented employment–screening procedure and

e. Procedures for regular evaluation of fraud risks and opportunities.

On the other hand, the management staff of the new and old generation banks differed significantly in their mean responses on the extent of utilization of the under listed corporate fraud control systems in the commercial banks:

a. Written operation procedure manual,

b. Written procedure for regular credit evaluation, supervision and monitoring, and

c. Standard system for fraud education and awareness campaigns.

HO_2: There was no significant difference in the mean responses of the management staff of new and old generation banks on the extent of utilization of the following corporate fraud prevention systems in the commercial banks:

a. Electronic method of authentication and authorization of payments,

b. Credit and debit alert systems,

c. Overt and closed–circuit surveillance system,

d. Inter and intra banks connectivity systems,

e. Computerized system of monitoring bank transactions and

f. Firewall and data encryption technology.

On the other hand, there was significant difference in the mean responses of the management staff of old and new generation banks on the extent of utilization of database of fraudsters and suspected customers in the commercial banks.

HO_3: It was found that there was no significant difference in the mean responses of the management staff of the new and old generation banks on the effectiveness of the following corporate fraud control systems in the commercial banks:

a. Standard system for monitoring employee characteristics and spending patterns,

b. Documented employment–screening system,

c. Proper career development programmes for employees,

d. Proper method of posting, placement and disengagement of employees and

e. Internal and external auditing systems

The management staff of the new and old generation banks only differed significantly on the effectiveness of written operation procedure manual in controlling corporate frauds in the commercial banks.

HO_4: The findings pertaining to **HO_4** showed that the management staff of the new and old generation banks did not differ significantly in their mean responses on the effectiveness of the following corporate fraud prevention systems in preventing fraudulent activities in commercial banks:

a. Database of lost cheques and other banking instruments,

b. Credit and debit alert systems,

c. Web geolocation technology for locating internet users,

d. Overt and closed circuit surveillance systems and

e. Inter and intra banks connectivity systems.

However, there was significant difference in the mean responses of the management staff of the new and old generation banks on the effectiveness of the under listed corporate fraud prevention systems in preventing frauds in the banks:

a. Computer and accounting forensic systems and

b. Firewall and data encryption technology.

HO_5: There was no significant difference in the mean reponses of the management staff of new and old generation banks on the following problems faced by commercial banks in the utilization of the corporate fraud control and prevention systems:

a. high cost of acquiring and implementing the anti-fraud systems,
b. Collaboration of bank officials, staff and third parties to commit frauds,
c. Many incompetent systems operators,
d. Customers' and employees' poor perception of the anti-fraud systems and
e. Complexities and sophistication in the corporate fraud control and prevention systems.

Discussion of the Findings

The findings of this study are discussed according to the research questions and hypotheses as follows:

Research Questions

1. The findings pertaining to research question one revealed that many corporate fraud control systems were available in most commercial banks.

Some of them were suitable internal control systems, documented employment-screening procedure and written operation procedure manual. This finding is in consonance with Uwakwe (2003) that most commercial banks had in place many of the corporate fraud control and prevention systems. Ugwunna (1998) also stated that many commercial banks were found to have employed adequate number of fraud control and prevention measures.

It was also found that most of the commercial banks had regular evaluation of fraud risks and opportunity procedures. This is in line with Osasebor (2004) that commercial banks establish risk assessment, monitoring and supervision review procedures to control and prevent corporate frauds. It was also on the findings that suitable internal control system was available in most commercial banks for corporate fraud control.

2. It was found in research question two that most of the corporate fraud prevention systems were available in the commercial banks. Some of the available systems were electronic methods of authentication and authorization of payments. Smith (2000) in consonance with the above findings stated that commercial banks were offering real-time payment authentication and authorization for transactions above the specific floor limits. Nestor (1998) also stated that electronic payment authorization was one of the main strategies used by commercial banks to prevent debit and credit card frauds.

The findings further showed that computerized system for monitoring bank transactions was available in the commercial banks to prevent corporate fraudulent activities. Computer and accounting forensic systems and the up-gradation of the systems in commercial banks had helped immensely in bank fraud prevention. Shackell (2000) in support stated that commercial banks had

developed computer forensic systems in response to trends in corporate fraudulent activities. However, firewall and data encryption technology, biometric identifiers for identifying customers, and database of fraudsters and suspected customers were found not available in the commercial banks. Overt and closed-circuit systems were also not available in the commercial banks.

3. The findings on research question three showed that most of the corporate fraud control systems were utilized most times in the commercial banks. Standard system for reward and punishment of employees was among the systems found to be utilized most times by the commercial banks to control fraudulent activities. This finding was in line with Bhaskar (2006) that commercial banks review on regular basis the operation of their staff and report on defaulters and take appropriate measures on them to improve their services. He stated that the banks put detailed quarterly analysis of all bank related complaints to their top management for appropriate action.

It was also found that the commercial banks most times utilized internal and external auditing systems in their corporate fraud control and prevention. The above finding was in agreement with Aderibigbe (1999) that commercial banks should have functional internal audit department to promote the efficiency of staff. He further stated that a qualified accountant should head the internal audit department to ensure effectiveness. It was also found that commercial banks often utilized the system of monitoring employee characteristics and spending patterns. This is to ensure that the character and behaviour of employees are in line with the laid down objectives of the organization. Other corporate fraud control systems utilized in the commercial banks were standard system for fraud education and awareness campaigns,

regular evaluation of fraud risks and opportunities as well as proper method of posting, placement and disengagement of staff.

4. As regards the extent of utilization of the corporate fraud prevention systems in commercial banks, it was found that electronic method of authentication and authorization of payments was utilized most times in the commercial banks. This method was utilized to ensure that payments are made to the true owners of bank accounts according the rules and regulations guiding bank transactions. Charlton and Taylor (2004) identified electronic authentication and authorization as the most basic techniques utilized by commercial banks for fraud prevention in the banking environment. This process verifies that the money-withdrawing instrument like plastic cards and cheques are valid and has sufficient fund attached to them in the account. Other corporate fraud prevention systems found to be utilized most times in the commercial banks were credit and debit alert systems, password technology, challenge-response and call-back protocols.

Some of the corporate fraud prevention systems were found to be utilized often in the commercial banks. Those systems utilized often in the banks include: web geolocation technology, overt and closed-circuit systems, computer and accounting forensic systems as well as inter and intra banks connectivity systems. It was also found that biometric identifiers were often utilized in the commercial banks to identify customers. The above finding is in agreement with Johnson (1999) that biometric identification systems that make use of an individual's unique physical characteristics like fingerprints, voice patterns, retinal images, etc were often used by commercial banks. Although some of the corporate fraud prevention systems were utilized most times while

some were utilized often in the banks none of the systems was utilized always, sometimes or seldom in the commercial banks.

5. With regard to the effectiveness of the corporate fraud control systems in the commercial banks, it was found that many of the systems were effective in controlling fraudulent activities in the commercial banks. Internal and external auditing systems were found to be effective in controlling fraudulent activities in the banks. The above findings support Graycar (2004) that the basic elements of an effective corporate fraud control systems include regular auditing of transactions by an internal auditor backed up by independent and accountable external auditors. He stated that the first line of defence against complex corporate fraud was to ensure the greatest possible transparency of corporate transactions through effective internal and external auditing systems.

It was also found that proper career development programmes organized for employees were effective in controlling fraudulent activities in the commercial banks. The findings also showed that written operation procedure manual and written procedure for credit evaluation; supervision and monitoring were effective in corporate fraud control in the commercial banks. The above findings are in consonance with Aderigigbe (1999) that commercial banks have written operating procedure manual as well as functional internal audit department to promote the effectiveness and efficiency of both staff and management. None of the corporate fraud control systems was found to be ineffective in corporate fraud control in the commercial banks.

6. With regard to the effectiveness of the corporate fraud prevention systems in the commercial banks, it was found that electronic method of authorization was effective in the prevention of frauds in the commercial banks. The above

finding agreed with Damagun (2003) that effectiveness of corporate fraud prevention systems would be ensured if the systems provide for authorization of transactions, proper documentation and classification of transactions. Separation of duties and supervision of transactions should also be assured.

Other corporate fraud prevention systems found to be effective in preventing fraudulent activities in the commercial banks included biometric identifiers, overt and closed-circuit surveillance system, credit and debit alert systems as well as password technology, challenge-response and call-back protocols. According to Okauru (2007) all the above financial policies and operations are aspects of "know Your Customer (KYC)" procedures developed by commercial banks as anti-fraud solutions. He stated they are effective in bank fraud prevention.

7. As it concerned the problems faced by commercial banks in the utilization of the corporate fraud control and prevention systems, the findings showed that customers' and employees' poor perception of the systems usually affected the successful implementation of the anti-fraud systems. The above finding was in agreement with Charlton and Taylor (2004) that the effectiveness of corporate fraud control and prevention systems in commercial banks depended on the perception and attitudes of the bank customers and staff. The American Institute of Certified public Accountants (AICPA, 2002) stated that when employees and customers have positive feelings or perception about an organization and its systems, corporate frauds occur less frequently than when they (the customers and employees) feel abused, threatened or ignored.

It was also found that proper implementation of the corporate fraud control and prevention systems in the commercial banks was limited by

collaboration of bank officials, staff and third parties. The above finding was in consonance with Aguolu (2002) that the limitation of the effectiveness of fraud control systems included staff and third party collusions and abuse of authority by people in management. The findings pertaining to the problem encountered in the utilization of the corporate fraud control and prevention systems in the commercial banks also included instability in power supply, heavy workload, complexity and sophistication of the corporate fraud control and prevention systems. These factors threaten the effective utilization of the anti-fraud systems in the commercial banks.

8. Pertaining to the strategies for enhancing the effective utilization of corporate fraud control and prevention systems in commercial banks, it was found that specialized training, seminars and workshops should be organized regularly for both the staff and management. Jenfa (2002) in his own opinion was in agreement with the above findings that the institutional factors that affected the systems included inadequate training and retraining of staff on both technical and theoretical aspects of the systems. According to Jenfa, failure by both the management and staff to undergo on-the-job training and even relevant outside courses lead to unsatisfactory performance which eventually creates more room for malpractices.

It was also found that sustainable programmes for continuous education and awareness of all bank stakeholders in fraud control and prevention should be maintained. The above findings were as stated by Ngige (1999) that staff and customers of commercial banks should be constantly educated, trained and retrained in the operation and observance of corporate fraud control and prevention systems. As was found, more competent systems operators for the

corporate fraud control and prevention systems should be employed to reduce workloads and the errors that might occur. According to Ngige (1999) if the operation of the systems is in the hands of people who are not too skilled in the act, the people are often victims of incessant mistakes. They most times busy themselves with the rectifying of mistakes instead of developing initiatives and innovations. Other strategies identified for enhancing the effective utilization of the corporate fraud control and prevention systems in commercial banks include: employment of more competent operators for the systems, greater regulatory oversight functions, adequate and commensurate incentives for employees and well defined organizational structures.

Discussion Pertaining to the Hypotheses

HO_1: The test on HO_1 revealed that there was no significant difference in the mean responses of the management staff of new and old generation banks on the extent of utilization of the corporate fraud control systems in the commercial banks. The above findings implied that the corporate fraud control systems were utilized in similar extent in both the new and old generation banks. The above finding was in contrary to the view of Charlton and Taylor (2004) that the utilization of fraud prevention techniques was more popular in some banks than others. According to them some anti-fraud techniques were only applied by some banks after frauds have been experienced rather than as pre-emptive measure. One had expected that the age, location and capacity of a bank would have significant influence on the extent to which corporate fraud control systems were utilized in the bank.

HO_2: The findings made from the test carried on HO_2 showed that there was no significant difference in the mean responses of the management staff of new

and old generation banks on the extent of utilization of the corporate fraud prevention systems in the commercial banks. The above findings agreed with the United States of America delegation to the Inter government Expert Group (2006) that fraud control and prevention systems were widely utilized in most commercial banks without any regard to the age or location of the banks. However, the above findings were at variance with the views of Charlton and Taylor (2004) that some fraud prevention techniques were more popular in some banks than others with regard to the extent of their utilization in the commercial banks.

HO_3: It was found that there was no significant difference in the mean responses of the management staff of new and old generation banks on the effectiveness of the corporate fraud control systems in controlling frauds in the commercial banks. The null hypothesis of no significant difference was not rejected because the opinions of the management staff in both the new and old generation banks did not differ significantly with regard to the effectiveness of the fraud control systems in controlling frauds in the commercial banks. However the management staff of the new and old generation banks only differed significantly on one item which was the effectiveness of written operation procedure manual on controlling corporate frauds in the commercial banks.

HO_4: It was further found that there was no significant difference in the mean responses of the management staff in new and old generation banks on the effectiveness of database of lost cheques, credit and debit alert system, web geolocation technology, overt and closed-circuit surveillance systems in preventing corporate frauds in the commercial banks. It was also found that

there was no significant difference in the mean responses of the management staff on the effectiveness of inter and intra banks connectivity systems in preventing fraudulent activities in the commercial banks. The above findings implied that those fraud prevention systems mentioned above were effective in all the banks with little or no difference. However, there was significant difference in the mean differences of the management staff in new and old generation banks on the effectiveness of computer and accounting forensic systems, and firewall and data encryption technology. It implied that those systems could be more effective in some banks than others. The above findings agreed with Charlton and Taylor (2004) that the effectiveness and utilization of some fraud prevention systems were more popular in some banks than others.

HO_5: The test on HO_5 revealed that there was no significant difference in the mean responses of the management staff of new and old generation banks on the problems encountered by the commercial banks in the utilization of the corporate fraud control and prevention systems. The implication of the above findings was that the problems of corporate fraud control and prevention systems, which existed in the new generation banks, also existed in almost the same degree in the old generation banks. The null hypothesis of no significant difference was not rejected because the opinions of the management staff in both the new and old generation banks did not differ with regard to the problems encountered by the commercial banks in the utilization of the corporate fraud control and prevention systems. The opinions of the management staff were in consonance with the United States of America Delegation to the Intergovernmental Exert Group (2006) that

fraud control and prevention systems were widely utilized in most commercial banks without due influence by the age or location of the commercial banks.

CHAPTER FIVE
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

This chapter presents the summary of the study, conclusions and recommendations.

Restatement of the Problem

Commercial banks are financial institutions that accept monetary deposits and effect withdrawals on demand by the depositors. The major services provided by commercial banks are the management of the nation's payment systems and fund transfers. However, commercial banks in Nigeria are highly vulnerable to various forms of frauds because of the recent computerization of bank products and services coupled with the huge financial assets handled by them. The recent use of computers, the internet and other electronic devices for banking services had made certain fraudulent activities more efficient, faster and easily concealed.

The number of commercial banks in Nigeria since 1892 when the first commercial bank was established in Nigeria has not increased steadily. This is because of intermittent bank failures mainly caused by frauds. The statistics of failed banks in Nigeria shows that the Central Bank of Nigeria between 1994 and 2006 revoked the licenses of about 50 commercial banks. Bank failure has resulted to poor image for most banks and low credibility to commercial banks in Nigeria. According to Karwai (2003), bank fraud is badly affecting every aspect of the banking system to the extent that many banks have lost the confidence of their customers. Consequently, foreign investment inflow into Nigeria is restricted. The banks lose billions of Naira every year due to fraudulent activities. Nigerian commercial banks lost more than N48 billion

between 2001 and 2006 to various forms of fraudulent activities (Aderinokun, 2007).

In order to stay afloat in their commercial activities, commercial banks install and utilize fraud control and prevention systems to fight the scourge of corporate frauds. However, the availability, the extent of utilization and the effectiveness of those systems need to be ascertained. This is necessary because of the amount of frauds occurring in the banks recently. It was also suspected that the problems of lack of adequate infrastructure and skilled manpower among others affected commercial banks' effective operations. The above problems must have also militated against the efficient utilization of the systems in most commercial banks. The identification of the strategies for enhancing the effective utilization of the corporate fraud control and prevention systems was, therefore, a necessity. Based on the foregoing, this study was undertaken to determine the corporate fraud control and prevention systems in commercial banks in Enugu State of Nigeria.

Summary of the Procedure Used

The study adopted a survey research design. Eight research questions were answered while five null hypotheses were tested at 0.05 level of significance. The population of the study comprised all the 288 management staff in the 96 commercial bank branches operating in Enugu State. The entire population was used for the study because it was manageable. Three management staff from each of the 96 commercial bank branches made up the 288 management staff used for the study. The management staff were the manager, the accountant and the supervisor of each of the commercial bank branches. The research instrument used was structured questionnaire. The

questionnaire contained 97 items. The questionnaire was subjected to face validation by three specialists from the Department of Vocational Teacher Education, University of Nigeria, Nsukka and two professional Accountants in the Service of University of Nigeria, Nsukka. Kuder–Richardson (K-R20) Reliability coefficient of 0.96 and 0.99 were obtained for the questionnaire items in sections B and C of the questionnaire respectively while Cronbach Alpha Reliability Coefficient of 0.99, 0.98, 0.98, 0.99, 0.99 and 0.98 were obtained for the other six clusters in sections D to I of the questionnaire respectively. The questionnaire was administered personally by the researcher with the help of two trained research assistants. 288 copies of the questionnaire were administered but 257 copies or 89 percent of the copies were returned and analysed for the study. Research questions one and two were answered using frequencies and percentages while research questions three to eight were answered using the mean and standard deviation. The null hypotheses one to five were tested using t–test statistic at 0.05 level of significance. Special Package for the Social Sciences (SPSS) was used to analyze the data collected for the study.

Summary of Findings

The findings of the study are summarized according to the research questions and hypotheses as follows:

Research Questions:

1. It was found that some of the corporate fraud control systems were available in the commercial banks. Those corporate fraud control systems that were

available included written operation procedure manual and documented employment screening procedure manual.

2. With regard to the availability of the corporate fraud prevention systems, it was found that many of the corporate fraud prevention systems were available in the commercial banks. They included electronic method of authentication and authorization of payment systems, and credit and debit alert systems.

3. On the extent of utilization of the corporate fraud control systems, it was found that the commercial banks utilized the corporate fraud control systems most times. Some of the mostly utilized systems were suitable internal control system and standard system for monitoring employee characteristics and spending patterns.

4. The findings on the extent of utilization of the corporate fraud prevention systems showed that the corporate fraud prevention systems were most times utilized in the commercial banks. Password technology, challenge–response and call–back protocols were among the corporate fraud prevention systems utilized most times in the commercial banks.

5. It was found that most of the corporate fraud control systems utilized in the commercial banks were effective in controlling corporate fraudulent activities. Proper career development programmes for employees, written operation procedure manual as well as internal and external auditing systems were found to be effective in controlling corporate frauds in the commercial banks.

6. Most of the corporate fraud prevention systems were found to be effective in preventing corporate fraudulent activities in the commercial banks. Some of the systems found to be effective in preventing fraudulent activities in the

commercial banks were credit and debit alert systems, password technology, challenge response and call–back protocols.

7. It was found that the commercial banks encountered many problems in the utilization of the corporate fraud control and prevention systems. The problems encountered included instability in power supply, complexity and sophistication in the systems together with unskilled systems operators.

8. It was also in the findings that effective utilization of the corporate fraud control and prevention systems could be enhanced by the employment of more competent operators of the systems with commensurate incentives and the regular organization of sustainable programmes for fraud education and awareness for all bank stakeholders.

Hypotheses

Ho_1: It was found that there was no significant difference in the mean responses of the management staff in new and old generation banks with regard to the extent of utilization of the corporate fraud control systems in the commercial banks.

Ho_2: It was also found that there was no significant difference in the mean responses of the management staff in new and old generation banks with regard to the extent of utilization of the corporate fraud prevention systems in the commercial banks.

Ho_3: There was no significant difference found in the mean responses of the management staff in new and old generation banks with regard to the effectiveness of the corporate fraud control systems in the commercial banks.

Ho_4: There was no significant difference found in the mean responses of the management staff of new and old generation banks with regard to the

effectiveness of corporate fraud prevention systems in preventing fraudulent activities in the commercial banks.

Ho_5: No significant difference was found in the mean responses of the management staff of new and old generation banks with regard to the problems encountered by commercial banks in the utilization of the corporate fraud control and prevention systems.

Implications of the Findings for Business Education

The findings of this study have the following positive implications for Business Education:

1. The findings of this study especially about the availability, the extent of utilization and the effectiveness of the corporate fraud control and prevention systems in commercial banks would induce business educators to stress the importance and strengths of corporate fraud control and prevention systems to their students, bank customers, investors and other stakeholders of commercial banks.

2. The result of this study about the extent of utilization, the effectiveness and the problems militating against the effective utilization of the corporate fraud control and prevention systems in commercial banks would enhance business educators' understanding and teaching of corporate fraud control and prevention in public and private organizations in general, and commercial banks in particular.

3. Business educators would use the facts of the findings of this study as a bench mark for guiding and counseling bank customers, investors and other stakeholders of commercial banks on how to handle their banking services and transactions to avoid fraudulent activities and the adverse effects.

4. The findings of this study would help business educators to clear the misconceptions held by many members of the public including bank customers and investors on the establishment and utilization of corporate fraud control and prevention systems in commercial banks. This would instill more confidence in the customers and investors, and hence guarantee their patronage of commercial banks. The business of the banks would greatly increase.

5. Curriculum experts in Business Education would use the findings of this study in the planning, review and update of the Business Education curriculum especially as it affects corporate fraud control and prevention.

6. Business Educators would also use the findings of this study especially as they affect the problems encountered in the utilization of the corporate fraud control and prevention systems to assist the management of commercial banks in the training and research for effective utilization of corporate fraud control and prevention systems.

Conclusions

Conclusions for this study were made based on the findings of the study. The conclusions were drawn from the findings on the availability, the extent of utilization and the effectiveness of the corporate fraud control and prevention systems in the commercial banks. Conclusions were also drawn from the findings on the problems encountered by the commercial banks and the strategies for enhancing the effective utilization of the corporate fraud control and prevention systems in the commercial banks.

It was concluded from the findings of the study that some of the corporate fraud control and prevention systems were available in the commercial banks. Although some of the corporate fraud control and

prevention systems were available in the banks, the systems were inadequately available in the banks. This might be because of the problem posed by the high cost of acquiring the corporate fraud control and prevention systems.

Secondly, it was concluded that the corporate fraud control and prevention systems were not always utilized in the commercial banks. The corporate fraud control and prevention systems were not extensively utilized in the commercial banks because of many problems associated with the utilization of the anti-fraud systems. Such problems include: complexity and sophistication in the systems as well as incompetent operators that handle the systems. The high cost of training the personnel for the operation of the complex systems also contributed to the shortage of personnel for effective utilization of the systems.

Another conclusion made for the study was that most of the corporate fraud control and prevention systems in the commercial banks were effective in fraud control and prevention in the banks. However, none of the corporate fraud control and prevention systems was very effective. The effectiveness of systems may have been limited by under utilization of the systems which is mainly caused by certain problems. The problems include: management over-ride of controls, and customers and employees' poor perception of the anti-fraud systems. Collaboration of bank officials, bank staff and third parties together with errors that arise from heavy workload also rendered some of the corporate fraud control and prevention systems not very effective for corporate fraud control and prevention in the commercial banks.

Generally, it was concluded from the findings of this study that the management of the commercial banks encountered many problems in the

establishment and utilization of the corporate fraud control and prevention systems. The problems restricted the full utilization and the effectiveness of the systems. However, many strategies could be adopted to enhance the effective utilization of the systems. Some of the strategies include: specialized training, seminars and workshops for both the staff and management of the commercial banks. Employment of more competent operators, regular review and update of the corporate fraud control and prevention systems would also enhance the effective utilization of the systems in the commercial banks.

Recommendations

Based on the findings made and conclusions drawn from the study, the following recommendations were made:

1. The management of the commercial banks should ensure that the available corporate fraud control and prevention systems are utilized, maintained and updated for effective fraud control and prevention.

2. The management of commercial banks should endeavour to ameliorate the identified problems encountered by the commercial banks in the utilization of corporate fraud control and prevention systems with the necessary strategies.

3. The management of the commercial banks should regularly review and update the corporate fraud control and prevention systems to ensure that they are relevant, adequate and effectively utilized.

4. The Central Bank of Nigeria and other relevant authorities should intensify their efforts in the supervision and monitoring of the activities of commercial banks to ensure that they establish and effectively utilize relevant and adequate corporate fraud control and prevention systems for fraud avoidance and reduction.

5. The management of commercial banks should devote much more time and resources for research and training in corporate fraud control and prevention to keep pace with the best practices and emerging technologies in financial industries.

Suggestions for Further Research

The following suggestions were made for further research:

1. The present study should be replicated in commercial banks in other states of Nigeria.

2. An analysis of the corporate fraud control and prevention systems in Micro-Finance Banks in Nigeria should be conducted.

3. The extent of utilization of corporate fraud control and prevention systems in insurance companies in Nigeria should be conducted.

Limitations of the Study

Questionnaire was the main instrument for gathering data for this study. Since there is always a degree of error in the final analysis of the data gathered by means of questionnaire, this study was limited, therefore, to the degree of cooperation received from the respondents, their ability to interpret the items and their objectivity in answering the questions.

REFERENCES

Abagnale, F. (2005). *Identity Theft*, Paper Presented at The Financial Services (ISAC) Members Meeting, St. Petersbury, Florida, May 4.

Achaka, B.A. (2004). *Fraudulent Practices and Financial Regulatory Audit of Terminal Benefit of Employees, Tax Revenue And Monetized Allowance,* Paper Presented at the National Workshop Organized by ICAN at Hill Station Hotel Jos, 7-10 August.

Adeniji, A.A. (2004). *Auditing and Investigations,* Lagos: Value Analysis Consult Publishers

Aderibigbe, P. (1999). *The International Audit Functions and Fraud: Nigeria Case Study. ICAN News.* January-March Pp 12-14

Aderinokun, T. (2007). *Strong Performance in a Rising Market, Interim Report of Guaranty Trust Bank.* Lagos: Guaranty Trust Bank Plc.

Agbo, E.T. (1991). Frauds in the Nigerian Banking System: A case Study of Cooperative and Commerce Bank and Union Bank of Nigeria Ltd. Enugu. *Unpublished B. Sc. Thesis,* UNEC: Department of Accountancy.

Agu,C.C. (2008). Understanding the A.B.C of the Financial Systems, 42nd Inaugural Lecture. University of Nigeria, Nsukka.

Aigbokhaevbolo, O.M (2001). Frauds and Commercial Banks in Nigeria. *The Certified National Accountant, The Journal of Association of National Accountants of Nigeria* (ANAN), 10 (4) Pp.30-39

Agu, C. C. (2008). Understanding the A.B.C. of Financial System. An Innaugural Lecture.of the University of Nigeria, Nsukka. Delivered at UNN.

Aguolu, O. (2002). *Fundamentals of Auditing.* Enugu: Meridian Associates

AICPA (2001). *Management Anti-Fraud Programmes and Controls*, New York: American Institute of Certified Accountants.

Akwaja, C. (2007). Organizations Have Lost Money to Poor Network Security, *Financial Standard Newspaper*. Lagos: Millennium Harvest Ltd. June 25, P. 46

Anyafo, A.M.O (2004). *Managing The Internal Control Systems,* Paper Presented At The N.B.C.B.S Workshop On Internal Control System Principles, Benefits And Hindrances For Internal Auditors Of Community Banks, N.B.C.B. Enugu, 26th-27th May.

Anyanwokoro, M. (1998), *Banking Methods and Procedures*. Enugu: Hosanna Publisher Ltd.

Ataman, P.A.H. (2007), *Welcome Address Presented at The One-Day Sensitization Workshop On Anti-Corruption And Transparency Organized By CBN,* Transparency, A Publication of CBN, 1 (1), June Pp 1-6.

Ataman, P.A.H.(2007). The Anatomy of Advance Free Frauds: Forms, Victims and Preventive Measures. *Transparency,* A Publication of CBN, 1(I) June Pp 34-42

Avey, T. (2004). Fraud and Commercial Fraud Prevention. *The CPA Handbook,* Toronto: America Institute of Certified Public Accountants

Ancxiom and Transunion (2004). *How Financial Institutions can overcome Identity Theft Challenges,* White Paper Released. Chicago; Ancxiom Corporation.

Banard, C. (1938). *The Functions of the Executive.* Cambridge, MA, USA: Harvard University Press.

Bank of Netherlands (2006). *General Policy Memorandum on Management of Computer Risk for Senior Management.* Attillen: The Bank of Netherlands.

Bhaskar, P.U. (2006). Credit Card Operation in Banks, *Master Circular to All Scheduled Commercial Banks.* India: Resserves Bank of India.

C.B.N (2006). *Annual Report on Commercial Banks.* Lagos: Central Bank of Nigeria

Chambers Harrap Publishers Ltd. (2006). *The Chambers Dictionary*, New Delhi: Allied Chambers (India) Ltd.

Charlton, K. And Taylor,N. (2004). Online Credit Card Fraud against Small Business, *Research and Public Policy Series Number 60.* Canberra: Australian Institute of Criminology.

Clark, R. (1998). *Information Technology and Dataveillance,* Australia: National University Academic Press

Cole, R. And Cumming, C.(1998). *Framework for Internal Control Systems in Banking Organizations*, Basle: Basle Committee on Banking Supervision, Available at Http://Www.Bis.Org/Pub/Bcbs 40.Pbs Accessed 13/08/04.

Damagun, Y. M. (2003). Effective Internal Control for Fraud Detection. *The Certified Natioal Accountant, Journal of ANAN* 11(2) June. PP. 50-53.

Ekine, A. (2008). Post Consolidation: Banking Perspectives and Players promise, *Sunday punch newspaper*, Lagos: Punch Publishing Company Ltd. August 17

Eze, C. (2006). An Assessment of Internal Control System in Community Banks in Enugu and Anambra States. *Unpublished Ph. D Thesis*, UNN:Department of Vocatioal Teacher Education

Farell, B.R. And Franco, J.R. (1999). The Role Of Auditors In The Prevention And Detection Of Business Fraud, *Western Criminology Review* 2(1) Pp 22-23. Available At Http.//Www. Wcr. Sovioma. Ed/V2n1 Htme. Accessed 24/4/2008

Fayol, H. (1949). *General Industrial Management.* London: Pitman.

Graycar, a (2004). *Fraud Prevention And Control.* Paper Presented at The Two-Day Conference On Fraud Prevention And Control. Gold Coast Australia, 24th-25th August, Available At Http://Www.Gov.Au/Conference/Fraud/Index.Html Accessed On 12/4/08

Ikegbuna, C.I. (1998). National Assessment Of Educational Progress In Nigeria, In G.A. Badmus and P.I. Odo (Eds) *Challenges of Managing Educational Assessment In Nigeria, N*igeria: JAMB, NABTEB and NBEM

Ile, N.M. (1999). *Management And Organizational Theory And Practice (2nd Ed).* Onitisha: Cape Publisher International Ltd.

Jenfa, B.I. (2002) Internal Control and Fraud Prevention: Accountants Perspective, *The Cerfified National Accountant, Journal Of Association Of National Accountants Of Nigeria (ANAN)*. 10 (4) Pp 30-39.

Johnson, E. (1999). Body of Evidence: How Biometric Technology Could Help in the Fight against Crime, *Crime Prevention News,* Australia; Australia Institute of Criminology, December Pp 17-19

Kalu, V.U. (2009). Financial Mess: How Nigeria Was Looted Blind, Saturday Sun Newspaper, Lagos: The Sun Publishing Ltd., August 22

Kama, I.U. (2003), The Constraints and Prospects of Effective Financial Surveillance in Nigeria, *Seminar Issue In Financial Institutions Surveillances in Central Bank of Nigeria*, Lagos: CBN Training Centre.

Kanu, A. N. (2004). Fraud and Its Management in Nigerian Banks: A Case Study of Union Bank of Nigeria Plc. *Unpublished B. Sc. Thesis,* UNEC: Department of Accountancy.

Karwai, S. A. (2003). *Bank Fraud: Can sharia Prevent It.* Conference Paper Presented at Ahmadu Bellow University, Zaria.

KMPG (2006), *Fraud Risk Management.* Survey Conducted By KMPG International.

Koontz, H. & O'Donnel C. (1972). *Principles of Management: an Analysis of Management Functions.* New York, Mc Graw-Hill Book Co.

Levy, I. (1999). Financial Fraud, *Wall Streets Journal*, New York, April 25th, 1(1) Pp 22-23.

Linnitt, M. (2006). *Credit Card Fraud in Indonesia,* Indonesia: Pt. Hill Konsultan

Mauria, S. (2001). *Prevention of Fraud under Computerized Environment,* Mubai: Banks Training College, Reserved Bank of India.

Mayo, E. (1933). *The Human problems of Industrial Civilization.* New York: Routledge.

Mbamalu, A.A. (2004). Management of Fraud in the Nigeria Commercial Banks (A Survey Of Selected Banks in Nnewi), *Unpublished MBA Thesis,* UNEC: Department Of Management.

Mintzberg, H. (1983). *Power in and Around Organizations.* Englewood Cliffs: Prentice-hall.

NDIC (2007). *Annual Report and Statement of Accounts*. Abuja: Nigerian Deposit Insurance Corporation.

Nduka,D.U. (2001). Effectiveness of The Internal Control Method as A Tool For Preventing Bank Fraud (A Case Study Of Five Commercial Banks), *Unpublished MBA Thesis,* UNEC: Department Of Banking And Finance.

Nestor Inc. (1998). Proactive Fraud Risk Management: Neural Network Credit Card Fraud Detection, *Available at Http://www.Nestor.Com/Rmd.Html Accessed On 6/4/2007*

Ngige, L.N. (1999). Fraud and Its Control: A Critical Analysis Of Computer Usage In Banks. *Unpublished MBA Thesis,* UNEC: Department Of Accountancy.

Ning. S. (2007). *Online Verification of Citizens Identity Information,* Press Conference Delivered, China: Peoples Bank Of China.

Nwofor, N.E. (2006). Bank Fraud And The Nigeria Economy (1991-Date): A Case Study Of Selected Commercial Banks In Enugu State Of Nigeria,

Unpublished MBA Thesis, University Of Nigeria, Enugu Campus: Department Of Banking And Finance.

Nwude, C. (2006). Bank Fraud, *The Nigerian Banker (Journal Of The Chartered Institute Of Bankers Of Nigeria, (NIBN)* October-December, P.7.

Nzekwu, R.A. (1999). An Examination of Manual and Computer- Aided Fraud Techniques in Nigeria Banking System (A Case Study Of Union Bank Of Nigeria Plc). U*npublished MBA Thesis*, UNEC: Department Of Banking And Finance

Obi, C.A. (2002). *Elements of Business*, Owerri, Nigeria: Cape Publisher International Ltd.

Ochejele, J.J. (2004). *Internal Control System and Fraud Management In Banks And Other Financial Institutions*. Paper Presented at The Workshop on Fraudulent Practices, Financial irregularities And Economic Crimes Prevention Detection and Control. Organized By ICAN, Jos Distict, 7-10th September.

Ogbulie, N. (2007). Hi-Tech Banking: Shared Ambition And Shared Opportunity: *Business World*, Lagos: Business World Communication Limited. April 2007.P.

Ohazuluike, S, (2001). *Internal Auditing.* Paper Presented at NBCB Workshop On Security Management For Managers Of Community Banks In Enugu Zone, Enugu 4th-5th July

Ohia, L. U. (1997). Internal Control and Fraud Prevention in Merchant Banks: A Case Study of Stanbic Merchant Bank Nig. Ltd. *Unpublished MBA Thesis*, UNEC: Department of Accountancy.

Ojuri, G. (2007). *Post Consolidation: Technological Integration To Drive Banks Competitiveness*, Paper Delivered at The Annual Information And Technology Summit In Lagos, August 10.

Okauru, A.B. (2007) Fighting Financial Crime In The Banking Sector In Nigeria: A Call For Concerted Approach. *Transparency. A Publication Of CBN,* 1(1) June Pp.56-61

Okeke, C. (2007). *Mortgage Financing And Asset/Liability Mismatch: The Way Out*. Paper Presented at The Two –Day Workshop Organized By Housing Corporation Of Nigeria ,Ogun State Chapter

Okereke, L.C. (2000). *Principles and Practice of Auditing and Investigation.* Lagos; Lima Publisher Ltd.

Onah, F.O. (2003). *Human Resource Management.* Enugu: Fulladu Publishing Company.

Onyekwelu, I.C. (1998). Corporate Strategies for Financial Risk Management in Banks. *Unpublished MBA Thesis,* UNEC: Department Of Banking And Finance.

Osasebor, J.O. (2004), *Pre-Emptive Strategies, Internal Control And Action Checklist On Fraud Detection, Prevention and Control*. Paper Presented At The 4-Day National Workshop Organized By ICAN Jos District 7-10 August.

Ossai, C.E. (2005). Effectiveness Of Internal Control in Fraud Prevention and Control in The Nigeria Patlic Sector (A Case Study of The Cash Centre of Delta State University Bursary Department at Abraka) *Unpublished MBA Thesis* UNEC: Department of Banking and Finance.

Osuala, E.C. (1998). *Fundamentals Of Marketing (2nd Ed)*. Onitsha: Cape Publisher International Ltd.

Osuala, E.C. (2004). *Teach Yourself Business Management*. Onitsha, Nigeria: African First Publisher Ltd.

Osuala, E.C. (2005). *Introduction to Research Methodology (4th Ed).* Enugu, Nigeria: Cheston Agency Ltd.

Osuala, E.C. (2006). *Administrative Office Management*. Enugu: Cheston Agency Ltd.

Ovuakporie, V. (1998). *Bank Frauds-Causes And Prevention: An Empirical Analysis*. Ibadan: ATT Books Publisher Ltd.

Quova Inc (2005), Geolocation-Fraud Prevention for Online Financial Services. *Available At Http://www. Antiphising. Org/Sponsors Technical- Paper/Fsv. Frauds W P-2.10.05. Pdf* Accessed on 4/2/08.

Rauta, B. T. (1992). Internal Control and Fraud Prevention in Commercial banks, *Unpublished MBA Thesis,* UNEC: Department of Accountancy.

Reviere, R. (2004). School Effectiveness and School Change in Developing Countries e.g. Cape Verde. *Unpublished Ph.D. Thesis*. Dresden,Maputo,Mozanbique: University of Technology, Dresden.

Reynolds, G. D. (2006). Facial Recognition: A Biometric for the Fight against Cheque Fraud. *Journal of Economic Crime Management*, Wells Fargo Bank 4(2) Pp1-34.

Sanusi, J. (2003), *Financial Fraud, Money Laundering and Advance Fee Fraud.* Lagos: Central Bank Nigeria.

Sanusi, L. (2007). *Risk Management: Need To Minimize Risk Exposure,* Paper Presented at the 11th Annual Conference of Financial Correspondents and Business Editors, Organized By CBN At Enugu November, 2007

Shackell, M. (2002). *Corporate Fraud: Prevention, Detection and/Investigation, A Practical Guide to Dealing With Corporate Fraud.* Sydney: Pricewater House Coopers.

Smith, R.G. (1999). *Best Practice in Fraud Prevention,* Paper Presented At the 3rd National Outlook Symposium on Crime In Australia, Organized By The Australian Institute Of Criminology In Canberra 22-23 March

Smith, R.G. (2000), *Confronting Praud in The Digital Age*, Paper Presented at The Fraud Prevention And Control Conference Organized by The Australia Institute Of Criminology in Surfers Paradise 24-25 August.

Soludo, C. (2007), *Good Corporate Governance In Banks,* Paper Presented at the 11th Annual Conference for Finance Correspondence and Business Editors Organized by CBN at Enugu. November, 2007.

StanbicIBTC Bank (2008). *Equities Research: Special Report on the Nigerian Banking Industry*, Lagos: Stanbic IBTC Bank Plc.

Ugwunna, S.E. (1999), Fraud In The Nigeria Banking Industry: An Accounting Solution. *Unpublished MBA Thesis.* UNEC: Department of Accountancy.

Umeh, E.C. (2001). The Role of Management in Fraud Detection And Control: A Comparative Study of Two Public and Two Private Organizations in Enugu. *Unpublished MBA Thesis*. UNEC: Department of Accountancy.

United States Accounting Office (2002). Extent of Money Laundering and Credit Card Fraud, *Report Of The Chairman, Permanent Sub-Committee On Investigations,* Committee on Government Affair, U.S. Senate.

United State Delegation on Intergovernmental Affairs (2006). *Fraud and Criminal Misuse and Falsification of Identity.* Washington D.C: Intergovernmental Expert Group.

Usman, Z.B. (2004). *Fraud Indicators, Fraudulent Practices and Uncovered fraud in core Activities Areas,* Paper Presented During A 4-Day National Workshop on fraudulent Practices and Financial Irregularities. Organized by ICAN, Jos District 7-10 August

Uwakwe,G.M. (2003). The Impact of Internal Control on Corporate health of Nigerian Banks. *Unpublished MBA Thesis.* UNEC: Department of banking and Finance.

Uzoagulu, A. E. (1998). *Practical Guide to Writing Research Reports in Tertiary Institutions,* Enugu: John Jacob's Classic Publishers Ltd.

Vittal,N.(1999).*Information Technology and Emerging Challenges In The New Millennium For Banks.* Talk Delivered In the Bank Of Baroda Seminar, Mubai. 8th August,

Weber, M. (1947). *The Theory of Social and Economic Organization*. Glencoe 111, Free Press.

Wehemeier, S. (2001). *Oxford Advanced Learners Dictionary of Current English.* Oxford: Oxford University Press.

Wells Fargo Bank (2003). *Merchant Techniques For Advanced Fraud Protection*, White Paper Released. *Available at* Http://Www.Phoenix *hecht. com/ treasury Resources (Pdf) Wellfargo-Fraud% 20 Paper/ Pdf* Accessed On 12/5/08.

Wells, J.T. (2004). New Approaches To Fraud Deterrence, *Journal of Accountancy,* A publication of America Institute of Certified Public sAccountants, AICPA, USA, 2(3) Pp.10-12

Wilhelm, P. A. F. (2005). Contingent Corporate Governance: A Reflection on Global Fraud and Power configuration. *Journal of Global Business and Technology,* Switzerland: University of St. Gallen. 1(1) pp. 1-8

Witman, M. (2003), Enemy at the Gate: Threats to Information Security, *Acm Journal of Communication,* Virginian Commonwealth. University USA 46(8) Pp.91-95

Zervos, K (1999). Responding to Fraud in The 1990s. *Conference Proceedings,* Canberra: Australia Institute Of Criminology.

3VR Security Inc. (2006). *Fraud Loss Prevention for Retail Banking,* White Paper Prepared, San Francisco, USA. *Retrieved From* Http://Www.3VR.Com/Files/ *banking% 20 White Paper Pdf* Accessed 14/4/08

APPENDIX 1

Dept. of Vocational Teacher Education,

University of Nigeria, Nsukka.

22nd November, 2008

Dear Respondent,

LETTER OF INTRODUCTION

I am a post graduate student in the above department. I am currently conducting a research on **Corporate Fraud Control and Prevention Systems in Commercial Banks in Enugu State, Nigeria**.

Your opinion is highly valued for the successful completion of this research work. Please indicate in the appropriate columns in the questionnaire your honest response to each item of the questionnaire.

This research work is strictly for academic purpose. You are hereby assured that the information you give will be treated with the utmost confidentiality and used solely for the purpose of this study.

Thanks for your anticipated cooperation.

Yours faithfully,

Ugwoke Ernest O.

QUESTIONNAIRE

Section A: General Information

Tick the option and complete the blank spaces appropriately as they apply to you and your bank.

A. Name of your bank _____

B. Branch:_____

C. Your job position

(i) Manager ☐

(ii) Accountant ☐

(iii) Supervisor ☐

D. Category of your bank:

(i) Old generation bank ☐

(ii) New generation bank ☐

Section B: Corporate fraud control systems that can be available in commercial banks.

Please indicate by checks in the appropriate column the availability or non- availability of the following corporate fraud control systems in your bank.

S/No	Item Statement	Available	Not Available
1	Written operation procedure manual		
2	Written procedure for regular credit evaluation, supervision and monitoring.		
3	Internal and external auditing systems		
4	Documented employment-screening procedure.		
5	Standard system for monitoring employee characteristics and spending patterns.		
6	Standard system for fraud education and awareness campaigns.		
7	Standard system for reward and punishment of employees.		
8	Proper career development programs for employees.		
9	Suitable internal control systems		
1o	Procedures for regular evaluation of fraud risks and opportunities		
11	Proper method of posting, placement and disengagement of staff.		
12	Provision for regular review and update of processes and structures		

Section C: Corporate fraud prevention systems that can be available in commercial banks.

Please, indicate by checks in the appropriate columns the availability or non- availability of the following corporate fraud prevention systems in your bank.

S/No	Item Statement	Available	Not Available
13	Electronic method of authentication and authorization of payments.		
14	Firewall and data encryption technology.		
15	Database of lost cheques and other banking instruments.		
16	Credit and debit alert systems		
17	Biometric identifiers for identifying customers.		
18	Web geolocation technology for locating internet users		
19	Computerized system for monitoring bank transactions		
20	Overt and closed- circuit surveillance systems.		
21	Password technology, challenge- response and call-back protocols		
22	Computer and accounting forensic systems.		
23	Inter and intra bank connectivity system		
24	Database of fraudsters and suspected customers.		

Section D: The extent of utilization of corporate fraud control systems in commercial banks.

Please indicate in the appropriate column the Extent of utilization of each of the following corporate fraud control systems in your bank.

Response Categories		Point
Always	(A)	5
Most times	(MT)	4
Often	(O)	3
Sometimes	(ST)	2
Seldom	(S)	1

S/No	Item Statement	A	MT	O	ST	S
25	Written down operating procedure manual					
26	Written down procedure for regular credit evaluation supervision and monitoring					
27	Internal and external auditing systems.					
28	Documented employment-screening procedure.					
29	Standard system for monitoring employee characteristics and spending patterns.					
30	Standard system for fraud education and awareness campaigns.					
31	Standard system for reward and punishment of employees					
32	Proper career development programmes for employees					
33	Suitable internal control system					
34	Procedures for regular evaluation of fraud risks and opportunities.					
35	Proper method of posting, placement and disengagement of staff.					
36	Provision for regular review and update of processes and structures.					

Section E: The extent of utilization of corporate fraud prevention systems in commercial banks.

Please, indicate in the appropriate columns the extent of utilization of corporate fraud prevention systems in your bank.

Response Categories		Points
Always	(A)	5
Most times	(MT)	4
Often	(O)	3
Sometimes	(ST)	2
Seldom	(S)	1

S/No	Item Statement	A	MT	O	ST	S
37	Electronic method of authentication and authorization of payments					
38	Firewall and data encryption technology.					
39	Database of lost cheques and other banking instruments.					
40	Credit and debit alert system					
41	Biometric identifiers for identifying customers.					
42	Web geolocation technology for locating internet users.					
43	Computerized system for monitoring bank transactions.					
44	Overt and closed-circuit systems					
45	Password technology. Challenge-response and call-back protocols.					
46	Computer and accounting forensic systems.					
47	Inter and intra banks connectivity systems.					
48	Database of fraudsters and suspected customers.					

SECTION F: Effectiveness of the corporate fraud control systems utilized in commercial banks.

Please, indicate in the appropriate columns the level of effectiveness or ineffectiveness of each of the following corporate fraud control systems in controlling fraud in your banks

Response	**Categories**	**Points**
Very effective	(VE)	5
Effective	(E)	4
Rarely effective	(RE)	3
Ineffective	(I)	2
Very ineffective	(VI)	1

S/No	**Item Statement**	**VE**	**E**	**RE**	**I**	**VI**
49	Written down operating procedure manual					
50	Written down procedure for regular credit evaluation, supervision and monitoring.					
51	Internal and external auditing systems.					
52	Documented employment-screening procedure.					
53	Standard system for monitoring employee characteristics and spending patterns.					
54	Standard system for fraud education and awareness campaigns.					
55	Standard system for reward and punishment of employees					
56	Proper career development programmes for employees					
57	Suitable internal control systems					
58	Procedures for regular evaluation of fraud risks and opportunities.					
59	Proper method of posting, placement and disengagement of staff.					
60	Provision for regular review and update of processes and structures.					

Section G: Effectiveness of the corporate fraud prevention systems utilized in commercial banks.

Please, indicate in the appropriate columns the level of effectiveness or ineffectiveness of each of the following corporate fraud prevention systems in preventing frauds in your bank.

Response	**Categories**	**Points**
Very effective	(VE)	5
Effective	(E)	4
Rarely effective	(RE)	3
Ineffective	(I)	2
Very ineffective	(VI)	1

S/No	Item Statement	VE	E	RE	I	VI
61	Electronic method of authentication and authorization of payments.					
62	Firewall and data encryption technology					
63	Database of lost cheques and other banking instruments.					
64	Credit and debit alert system					
65	Biometric identifiers for identifying customers					
66	Web geolocation technology for locating internet users.					
67	Computerized systems for monitoring bank transactions.					
68	Overt and closed- circuit surveillance system.					
69	Password technology, challenge-response and call-back protocols					
70	Computer and accounting forensic systems.					
71	Inter and intra bank connectivity system					
72	Database of fraudsters and suspected customers					

Section H: Problems commercial banks can face in the utilization of the corporate fraud control and prevention systems.

Please, indicate in the appropriate columns your level of agreement or disagreement with the following statements on the problems faced by your bank in the utilization of corporate fraud control and prevention systems.

Response Categories		**Points**
Strongly agree	(SA)	5
Agree	(A)	4
Slightly agree	(SA)	3
Disagree	(D)	2
Strongly disagree	(SD)	1

S/No	**Item Statement**	**SA**	**A**	**Sa**	**D**	**SD**
73	The cost of acquiring and implementing the anti-fraud systems is very high					
74	The cost of training personnel to operate the anti-fraud systems is very high					
75	Proper implementation of the systems is limited by collaboration of bank officials, staff and third parties to commit fraud.					
76	Heavy workload leads to errors that limit proper implementation of the systems.					
77	Many of the system operators are not competent.					
78	Instability in power supply affects the successful implementation of the systems.					
79	The large volume of data to be stored and retrieved poses a problem to proper utilization of the systems.					
80	The complexity and sophistication in the systems limit successful utilization of the systems.					
81	Successful implementation of the systems is limited by management over-ride of internal control.					
82	Unprofessional and unethical behaviours exhibited by both management and staff sometimes limits successful utilization of the systems.					
83	Customers' and employees' poor perception of the systems affects the successful implementation of the systems.					
84	Too many anti-fraud systems make implementation unwieldy.					
85	Unclearly defined aspects of my bank's organizational structure cause unnecessary delays in the implementation of the systems.					

Section I: Strategies for improving the effective utilization of the corporate fraud control and prevention systems in commercial banks.

Please, indicate in the appropriate columns your level of agreement or disagreement with the following statements on strategies for improving the effective utilization of corporate fraud control and prevention systems in your bank.

Response categories		**points**
Strongly agree	(SA)	5
Agree	(A)	4
Slightly agree	(Sa)	3
Disagree	(D)	2
Strongly disagree	(SD)	1

S/No	**Item Statement**	**SA**	**A**	**SA**	**D**	**SD**
86	Enough funds should always be set aside in the bank's budget for the installation and implementation of fraud control and prevention systems.					
87	Specialized training, seminars and workshops should be regularly organized for both staff and management.					
88	More competent Operators for the fraud control and prevention systems should be employed to reduce workload.					
89	Greater regulatory oversight is needed to check the excesses of both staff and management.					
90	Sustainable programmes for continuous education and awareness of all bank stakeholders in fraud control and prevention should be maintained.					
91	The organizational structure of the bank should be clearly defined and monitored to check manipulations by both management and staff.					
92	Single systems that can be used for many operations in fraud control and prevention should be used to reduce costs.					
93	The fraud control and prevention systems should be regularly reviewed and updated to match with emerging technologies.					
94	Adequate effort should be given to research and development in fraud control and prevention.					
95	Adequate and commensurate incentives should be given to system operators and other employees.					
96	An automatic alternative source of power supply should be installed to alleviate the problem of frequent power failure.					
97	The acquisition and implementation of the ant-fraud systems should be made tax-free by government.					

APPENDIX 2

Summary of Computation of Reliability Coefficient for the Instrument for Corporate Fraud Control and Prevention System in Commercial Banks

Items	Available	Not Available	P	Q	Pq	$(X-\bar{x})^2$
1	22	6	0.79	0.21	0.1659	1.3689
2	24	4	0.86	0.14	0.1204	0.6889
3	26	2	0.93	0.07	0.0651	8.0089
4	26	2	0.93	0.07	0.0651	8.0089
5	27	1	0.96	0.04	0.0384	14.6689
6	21	7	0.75	0.25	0.1875	4.7089
7	25	3	0.89	0.11	0.0979	3.3489
8	24	4	0.86	0.14	0.1204	0.6889
9	23	5	0.82	0.18	0.0979	0.0289
10	24	4	0.86	0.14	0.1204	0.6889
11	26	2	0.93	0.07	0.0651	0.0089
12	10	18	0.36	0.64	0.2304	173.4489
	$\sum$= 278				$\sum$ = 1.3745	215.6668
	$\bar{X}$ = 23.17					

Variance $(S^2) = \frac{215.6668}{12} = 17.97$

Standard Deviation = $\sqrt{17.97} = 4.2394$

K-R20 = $\frac{N}{N-1}\left(1 - \frac{pq}{S^2}\right)$

Where N = 28

$K = \frac{28}{27}\left(1 - \frac{1.3745}{17.97}\right) = \frac{28}{27}\left(1 - 0.0765\right)$

$= \frac{28}{27} \times \frac{0.924}{1} = 0.958$

Items	Available	Not Available	P	q	Pq	$(X-\bar{x})^2$
13	19	9	0.68	0.32	0.2176	18.0605
14	10	18	0.36	0.64	0.2304	175.5625
15	24	4	0.86	0.14	0.1204	0.5625
16	26	2	0.93	0.07	0.0651	7.5625
17	26	2	0.93	0.07	0.0651	7.5625
18	28	0	1.00	0.00	0.0000	22.5625
19	27	1	0.96	0.04	0.0384	14.0625
20	20	8	0.71	0.29	0.2059	10.5625
21	25	3	0.89	0.11	0.0979	3.0625
22	24	4	0.86	0.14	0.1204	0.5625
23	27	1	0.96	0.04	0.0384	14.0625
24	23	5	0.82	0.18	0.1476	0.0625
	$\sum$ =279				$\sum$=1.3472	$\sum$=274.2500
	$\bar{X}$ =23.25					

Variance $(S^2) = \frac{274.2500}{12} = 22.85$

Standard Deviation (S) = $\sqrt{22.85} = 4.7806$

$$K - R20 = \frac{N}{N-1}\left(1 - \frac{\sum pq}{S^2}\right)$$

$$K = \frac{28}{27}\left(1 - \frac{1.3472}{22.8500}\right) = \frac{28}{27}\left(1 - 0.0590\right)$$

$$= 0.941$$

$$= \frac{28}{27} \text{ X } \frac{0.941}{1} = 0.976$$

Section D

Case Processing Summary

		N	%
Cases	Valid	28	10.9
	Excluded[a]	229	89.1
	Total	257	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.985	.989	12

Section E

Case Processing Summary

		N	%
Cases	Valid	28	10.9
	Excluded[a]	229	89.1
	Total	257	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.979	.984	12

Section F

Case Processing Summary

		N	%
Cases	Valid	28	10.9
	Excluded[a]	229	89.1
	Total	257	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.979	.982	12

Section G

Case Processing Summary

		N	%
Cases	Valid	28	10.9
	Excluded[a]	229	89.1
	Total	257	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.987	.989	12

Section H

Case Processing Summary

		N	%
Cases	Valid	28	10.9
	Excluded[a]	229	89.1
	Total	257	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.986	.990	13

Section I

Case Processing Summary

		N	%
Cases	Valid	28	10.9
	Excluded[a]	229	89.1
	Total	257	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.979	.986	12

Overall

Case Processing Summary

		N	%
Cases	Valid	28	10.9
	Excluded[a]	229	89.1
	Total	257	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.997	.998	73

APPENDIX 3

Data Analysis for Corporate Fraud Control and Prevention Systems in Commercial Banks

Research Question 1

	Available Frequency	percentage	Not Available Frequency	percentage
Item1	213	82.87938	44	17.12062
Item2	230	89.49416	27	10.50584
Item3	190	73.92996	64	24.90272
Item4	221	85.99222	36	14.00778
Item5	164	63.81323	93	36.18677
Item6	208	80.93385	49	19.06615
Item7	214	83.26848	43	16.73152
Item8	194	75.48638	61	23.73541
Item9	225	87.54864	32	12.45136
Item10	187	72.76265	70	27.23735
Item11	223	86.77043	34	13.22957
Item12	206	80.15564	51	19.84436

Research Question 2

	Available Frequency	percentage	Not Available Frequency	percentage
Item13	235	91.43969	22	8.560311
Item14	98	38.1323	159	61.8677
Item15	194	75.48638	63	24.51362
Item16	238	92.607	19	7.392996
Item17	86	33.46304	171	66.53696
Item18	77	29.96109	180	70.03891
Item19	217	84.4358	40	15.5642
Item20	83	32.29572	174	67.70428
Item21	228	88.71595	29	11.28405
Item22	198	77.0428	59	22.9572
Item23	237	92.2179	20	7.782101
Item24	89	34.63035	168	65.36965

Research Question 3

	N	Mean	Std. Deviation
Item25	257	3.7354	1.08974
Item26	257	3.9105	.98612
Item27	257	3.9844	1.04944
Item28	257	3.8327	1.07857
Item29	257	2.9416	1.42539
Item30	257	3.2996	1.36635
Item31	257	4.0506	.77142
Item32	257	4.1518	.98640
Item33	257	3.9805	.81227
Item34	257	2.6420	1.29763
Item35	257	3.4864	1.03871
Item36	257	3.4553	1.43578
Overall Mean	257	3.6226	1.04601

Research Question 4

	N	Mean	Std. Deviation
Item37	257	4.0973	1.03185
Item38	257	3.7471	1.06902
Item39	257	3.9105	1.02877
Item40	257	3.9611	.89183
Item41	257	2.8482	1.06632
Item42	257	2.8288	1.06519
Item43	257	3.6848	1.02977
Item44	257	3.4475	.87397
Item45	257	3.9183	.99468
Item46	257	3.2257	1.10558
Item47	257	3.8482	1.13723
Item48	257	3.1712	1.04670
Overall Mean	257	3.5574	.95784

Research Question 5

	N	Mean	Std. Deviation
Item49	257	4.1167	.81609
Item50	257	4.0078	.99997
Item51	257	3.9572	.88505
Item52	257	3.6459	.93286
Item53	257	2.8755	1.03836
Item54	257	4.1595	.70284
Item55	257	4.4630	.74974
Item56	257	3.7860	1.08475
Item57	257	3.9377	.87277
Item58	257	4.1440	.95540
Item59	257	3.8016	.93307
Item60	257	4.3580	.82222
Overall Mean	257	3.9377	.83481

Research Question 6

	N	Mean	Std. Deviation
Item61	257	4.1556	.98777
Item62	257	4.2646	.90573
Item63	257	4.2840	.84840
Item64	257	4.0078	.92699
Item65	257	3.8911	.86816
Item66	257	4.0311	.91803
Item67	257	4.0506	.89779
Item68	257	4.1362	.99262
Item69	257	3.7276	.89034
Item70	257	4.0778	.87152
Item71	257	3.9689	1.06754
Item72	257	4.1323	.70017
Overall Mean	257	4.0606	.85011

Research Question 7

	N	Mean	Std. Deviation
Item73	257	3.8755	.86606
Item74	257	3.9300	.87665
Item75	257	3.7354	1.03079
Item76	257	3.6809	.89669
Item77	257	3.6304	.97605
Item78	257	4.1362	.68532
Item79	257	3.4086	.93144
Item80	257	3.9572	.88945
Item81	257	2.7899	.97358
Item82	257	2.9883	.92061
Item83	257	3.8249	.97452
Item84	257	3.0545	.80825
Item85	257	4.0078	.75515
Overall Mean	257	3.6169	.82652

Research Question 8

	N	Mean	Std. Deviation
Item86	257	4.3424	.87916
Item87	257	4.4591	.71758
Item88	257	3.8638	.68532
Item89	257	3.9611	.68354
Item90	257	4.0467	.91310
Item91	257	4.0311	.73355
Item92	257	3.3152	.82318
Item93	257	4.0506	.81572
Item94	257	4.3658	.85151
Item95	257	4.5486	.64239
Item96	257	4.0973	.75666
Item97	257	3.7510	.73967
Overalll	257	4.0694	.70383
Valid N (listwise)	257		

t-Test of Hypothesis 1

Group Statistics

	Category	N	Mean	Std. Deviation	Std. Error Mean
Item25	New Generation Bank	134	3.5373	1.03805	.08967
	Old Generation Bank	123	3.9512	1.10775	.09988
Item26	New Generation Bank	134	4.0672	.94350	.08151
	Old Generation Bank	123	3.7398	1.00684	.09078
Item27	New Generation Bank	134	3.8657	1.12250	.09697
	Old Generation Bank	123	4.1138	.95130	.08578
Item28	New Generation Bank	134	3.8881	1.05246	.09092
	Old Generation Bank	123	3.7724	1.10745	.09986
Item29	New Generation Bank	134	2.9776	1.37358	.11866
	Old Generation Bank	123	2.9024	1.48443	.13385
Item30	New Generation Bank	134	3.0224	1.47392	.12733
	Old Generation Bank	123	3.6016	1.17166	.10564
Item31	New Generation Bank	134	4.0373	.78909	.06817
	Old Generation Bank	123	4.0650	.75466	.06805
Item32	New Generation Bank	134	4.2090	.89337	.07718
	Old Generation Bank	123	4.0894	1.07892	.09728
Item33	New Generation Bank	134	3.8881	.84658	.07313
	Old Generation Bank	123	4.0813	.76387	.06888
Item34	New Generation Bank	134	2.6866	1.30596	.11282
	Old Generation Bank	123	2.5935	1.29208	.11650
Item35	New Generation Bank	134	3.4104	.99027	.08555
	Old Generation Bank	123	3.5691	1.08704	.09802
Item36	New Generation Bank	134	3.6493	1.33353	.11520
	Old Generation Bank	123	3.2439	1.51680	.13677
Overall	New Generation Bank	134	3.6032	1.03707	.08959
	Old Generation Bank	123	3.6436	1.05950	.09553

Independent Samples Test

		t-test for Equality of Means				
		t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Item25	Equal variances assumed	-3.092	255	.002	-.41391	.13386
Item26	Equal variances assumed	2.690	255	.008	.32733	.12166
Item27	Equal variances assumed	-1.903	255	.058	-.24815	.13038
Item28	Equal variances assumed	.859	255	.391	.11570	.13475
Item29	Equal variances assumed	.422	255	.674	.07517	.17828
Item30	Equal variances assumed	-3.467	255	.001	-.57924	.16706
Item31	Equal variances assumed	-.287	255	.774	-.02773	.09650
Item32	Equal variances assumed	.970	255	.333	.11952	.12319
Item33	Equal variances assumed	-1.915	255	.057	-.19324	.10090
Item34	Equal variances assumed	.574	255	.567	.09307	.16225
Item35	Equal variances assumed	-1.224	255	.222	-.15866	.12958
Item36	Equal variances assumed	2.279	255	.023	.40535	.17784
Overall	Equal variances assumed	-.309	255	.758	-.04040	.13085

t-Test of Hypothesis 2

Group Statistics

	Category	N	Mean	Std. Deviation	Std. Error Mean
Item37	New Generation Bank	134	4.1343	.98707	.08527
	Old Generation Bank	123	4.0569	1.08114	.09748
Item38	New Generation Bank	134	3.8507	1.03697	.08958
	Old Generation Bank	123	3.6341	1.09596	.09882
Item39	New Generation Bank	134	3.9627	.89616	.07742
	Old Generation Bank	123	3.8537	1.15718	.10434
Item40	New Generation Bank	134	4.0299	.89224	.07708
	Old Generation Bank	123	3.8862	.88894	.08015
Item41	New Generation Bank	134	2.8955	1.07093	.09251
	Old Generation Bank	123	2.7967	1.06324	.09587
Item42	New Generation Bank	134	2.8134	1.07723	.09306
	Old Generation Bank	123	2.8455	1.05607	.09522
Item43	New Generation Bank	134	3.5896	1.09827	.09488
	Old Generation Bank	123	3.7886	.94307	.08503
Item44	New Generation Bank	134	3.4627	.86413	.07465
	Old Generation Bank	123	3.4309	.88782	.08005
Item45	New Generation Bank	134	4.0672	.83349	.07200
	Old Generation Bank	123	3.7561	1.12601	.10153
Item46	New Generation Bank	134	3.3209	1.01567	.08774
	Old Generation Bank	123	3.1220	1.19140	.10742
Item47	New Generation Bank	134	3.8582	1.15135	.09946
	Old Generation Bank	123	3.8374	1.12624	.10155
Item48	New Generation Bank	134	3.0075	.99242	.08573
	Old Generation Bank	123	3.3496	1.07873	.09727
Overall	New Generation Bank	134	3.5827	.92624	.08002
	Old Generation Bank	123	3.5298	.99418	.08964

Independent Samples Test

		t-test for Equality of Means				
		t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Item37	Equal variances assumed	.600	255	.549	.07742	.12901
Item38	Equal variances assumed	1.628	255	.105	.21660	.13306
Item39	Equal variances assumed	.848	255	.397	.10903	.12853
Item40	Equal variances assumed	1.292	255	.198	.14367	.11122
Item41	Equal variances assumed	.741	255	.459	.09877	.13327
Item42	Equal variances assumed	-.241	255	.810	-.03210	.13326
Item43	Equal variances assumed	-1.552	255	.122	-.19907	.12824
Item44	Equal variances assumed	.291	255	.771	.03179	.10933
Item45	Equal variances assumed	2.531	255	.012	.31107	.12292
Item46	Equal variances assumed	1.444	255	.150	.19894	.13776
Item47	Equal variances assumed	.146	255	.884	.02081	.14228
Item48	Equal variances assumed	-2.648	255	.009	-.34213	.12919
Overall	Equal variances assumed	.442	255	.659	.05290	.11979

t-Test of Hypothesis 3

Group Statistics

	Category	N	Mean	Std. Deviation	Std. Error Mean
Item49	New Generation Bank	134	3.9627	.83537	.07217
	Old Generation Bank	123	4.2846	.76309	.06881
Item50	New Generation Bank	134	3.9701	1.04730	.09047
	Old Generation Bank	123	4.0488	.94828	.08550
Item51	New Generation Bank	134	4.0299	.84016	.07258
	Old Generation Bank	123	3.8780	.92847	.08372
Item52	New Generation Bank	134	3.5746	.94493	.08163
	Old Generation Bank	123	3.7236	.91706	.08269
Item53	New Generation Bank	134	2.7985	1.05331	.09099
	Old Generation Bank	123	2.9593	1.01947	.09192
Item54	New Generation Bank	134	4.1791	.68112	.05884
	Old Generation Bank	123	4.1382	.72796	.06564
Item55	New Generation Bank	134	4.4403	.69921	.06040
	Old Generation Bank	123	4.4878	.80333	.07243
Item56	New Generation Bank	134	3.7463	1.15483	.09976
	Old Generation Bank	123	3.8293	1.00578	.09069
Item57	New Generation Bank	134	3.8881	.93921	.08114
	Old Generation Bank	123	3.9919	.79441	.07163
Item58	New Generation Bank	134	4.1493	.97724	.08442
	Old Generation Bank	123	4.1382	.93498	.08430
Item59	New Generation Bank	134	3.8806	.92618	.08001
	Old Generation Bank	123	3.7154	.93669	.08446
Item60	New Generation Bank	134	4.3731	.77238	.06672
	Old Generation Bank	123	4.3415	.87618	.07900
Overall	New Generation Bank	134	3.9160	.84382	.07290
	Old Generation Bank	123	3.9614	.82766	.07463

Independent Samples Test

		t-test for Equality of Means				
		t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Item49	Equal variances assumed	-3.216	255	.001	-.32187	.10010
Item50	Equal variances assumed	-.629	255	.530	-.07863	.12501
Item51	Equal variances assumed	1.376	255	.170	.15180	.11033
Item52	Equal variances assumed	-1.280	255	.202	-.14895	.11634
Item53	Equal variances assumed	-1.242	255	.215	-.16084	.12952
Item54	Equal variances assumed	.465	255	.642	.04089	.08790
Item55	Equal variances assumed	-.507	255	.613	-.04751	.09376
Item56	Equal variances assumed	-.612	255	.541	-.08300	.13562
Item57	Equal variances assumed	-.952	255	.342	-.10381	.10900
Item58	Equal variances assumed	.092	255	.926	.01104	.11953
Item59	Equal variances assumed	1.420	255	.157	.16515	.11628
Item60	Equal variances assumed	.308	255	.758	.03167	.10285
Overall	Equal variances assumed	-.434	255	.664	-.04534	.10441

t-Test of Hypothesis 4

Group Statistics

	Category	N	Mean	Std. Deviation	Std. Error Mean
Item61	New Generation Bank	134	4.1642	.98251	.08488
	Old Generation Bank	123	4.1463	.99740	.08993
Item62	New Generation Bank	134	4.1045	1.00576	.08688
	Old Generation Bank	123	4.4390	.74818	.06746
Item63	New Generation Bank	134	4.2687	.86853	.07503
	Old Generation Bank	123	4.3008	.82913	.07476
Item64	New Generation Bank	134	3.9776	.98459	.08506
	Old Generation Bank	123	4.0407	.86269	.07779
Item65	New Generation Bank	134	3.8134	.95120	.08217
	Old Generation Bank	123	3.9756	.76247	.06875
Item66	New Generation Bank	134	3.9328	.99016	.08554
	Old Generation Bank	123	4.1382	.82308	.07421
Item67	New Generation Bank	134	4.0224	.91328	.07890
	Old Generation Bank	123	4.0813	.88330	.07964
Item68	New Generation Bank	134	4.1418	.96676	.08352
	Old Generation Bank	123	4.1301	1.02397	.09233
Item69	New Generation Bank	134	3.7537	.87948	.07598
	Old Generation Bank	123	3.6992	.90477	.08158
Item70	New Generation Bank	134	4.2388	.90262	.07797
	Old Generation Bank	123	3.9024	.80383	.07248
Item71	New Generation Bank	134	3.9925	1.06550	.09204
	Old Generation Bank	123	3.9431	1.07353	.09680
Item72	New Generation Bank	134	4.1194	.69417	.05997
	Old Generation Bank	123	4.1463	.70922	.06395
Overall	New Generation Bank	134	4.0442	.88474	.07643
	Old Generation Bank	123	4.0786	.81393	.07339

Independent Samples Test

		t-test for Equality of Means				
		t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Item61	Equal variances assumed	.144	255	.885	.01784	.12358
Item62	Equal variances assumed	-3.004	255	.003	-.33455	.11137
Item63	Equal variances assumed	-.303	255	.762	-.03216	.10613
Item64	Equal variances assumed	-.544	255	.587	-.06304	.11591
Item65	Equal variances assumed	-1.500	255	.135	-.16218	.10815
Item66	Equal variances assumed	-1.799	255	.073	-.20538	.11414
Item67	Equal variances assumed	-.525	255	.600	-.05891	.11227
Item68	Equal variances assumed	.094	255	.925	.01171	.12419
Item69	Equal variances assumed	.490	255	.625	.05454	.11134
Item70	Equal variances assumed	3.144	255	.002	.33637	.10699
Item71	Equal variances assumed	.370	255	.711	.04945	.13353
Item72	Equal variances assumed	-.308	255	.759	-.02694	.08759
Overall	Equal variances assumed	-.324	255	.746	-.03444	.10634

t-Test of Hypothesis 5

Group Statistics

	Category	N	Mean	Std. Deviation	Std. Error Mean
Item73	New Generation Bank	134	3.8358	.96708	.08354
	Old Generation Bank	123	3.9187	.74210	.06691
Item74	New Generation Bank	134	4.0224	.77038	.06655
	Old Generation Bank	123	3.8293	.97264	.08770
Item75	New Generation Bank	134	3.8507	.94596	.08172
	Old Generation Bank	123	3.6098	1.10612	.09974
Item76	New Generation Bank	134	3.5075	.96359	.08324
	Old Generation Bank	123	3.8699	.77839	.07019
Item77	New Generation Bank	134	3.6269	1.04537	.09031
	Old Generation Bank	123	3.6341	.89871	.08103
Item78	New Generation Bank	134	4.1866	.63917	.05522
	Old Generation Bank	123	4.0813	.73097	.06591
Item79	New Generation Bank	134	3.3582	.97644	.08435
	Old Generation Bank	123	3.4634	.88051	.07939
Item80	New Generation Bank	134	3.9552	.80287	.06936
	Old Generation Bank	123	3.9593	.97844	.08822
Item81	New Generation Bank	134	2.8209	1.01752	.08790
	Old Generation Bank	123	2.7561	.92631	.08352
Item82	New Generation Bank	134	3.0075	.88849	.07675
	Old Generation Bank	123	2.9675	.95758	.08634
Item83	New Generation Bank	134	3.8060	.92969	.08031
	Old Generation Bank	123	3.8455	1.02456	.09238
Item84	New Generation Bank	134	3.0149	.77542	.06699
	Old Generation Bank	123	3.0976	.84363	.07607
Item85	New Generation Bank	134	3.9627	.75996	.06565
	Old Generation Bank	123	4.0569	.74987	.06761
Overall	New Generation Bank	134	3.6119	.82261	.07106
	Old Generation Bank	123	3.6223	.83409	.07521

Independent Samples Test

		t-test for Equality of Means				
		t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Item73	Equal variances assumed	-.766	255	.445	-.08288	.10823
Item74	Equal variances assumed	1.772	255	.078	.19312	.10901
Item75	Equal variances assumed	1.882	255	.061	.24099	.12808
Item76	Equal variances assumed	-3.299	255	.001	-.36246	.10987
Item77	Equal variances assumed	-.060	255	.953	-.00728	.12212
Item78	Equal variances assumed	1.231	255	.219	.10527	.08549
Item79	Equal variances assumed	-.904	255	.367	-.10521	.11635
Item80	Equal variances assumed	-.037	255	.970	-.00413	.11128
Item81	Equal variances assumed	.532	255	.595	.06480	.12174
Item82	Equal variances assumed	.347	255	.729	.03998	.11516
Item83	Equal variances assumed	-.325	255	.746	-.03956	.12190
Item84	Equal variances assumed	-.818	255	.414	-.08264	.10099
Item85	Equal variances assumed	-.999	255	.319	-.09422	.09430
Overall	Equal variances assumed	-.100	255	.921	-.01032	.10341

APPENDIX 4

LIST OF COMMERCIAL BANK BRANCHES OPERATING IN ENUGU STATE

ACCESS BANK PLC

1. 46 Ogui Road Branch, Enugu

2. 67 Ogui Road Branch, Enugu

AFRIBANK PLC

3. 36 Okpara Avenue Branch, Enugu

4. Plot 38 Okpara Avenue Branch, Enugu

5. IMT/Emene Road Branch, Enugu.

6. Timber Shed Branch, Enugu

7. 40 Ogui Road Branch, Enugu

BANK PHB PLC

8. 34 Zik Avenue Branch, Enugu

9. 23 Okpara Avenue Branch, Enugu

10. Plot 7 Pocket Layout Branch, Enugu

11. Enugu Road Branch, Nsukka.

DIAMOND BANK PLC

12. Okpara Avenue Branch, Enugu

13. Garden Avenue Branch, Enugu

14. Enugu/Orba Road Branch, Nsukka

15. UNN Branch, Nsukka

ECOBANK PLC

16. 20B Okpara Avenue Branch, Enugu

17. UNEC Branch, Enugu

18. 31 Okpara Avenue Branch, Enugu

EQUITORIAL TRUST BANK PLC

19. Ogui Road Branch, Enugu

20. 23 Okpara Avenue Branch, Enugu

FIDELITY BANK PLC

21. Ogui Road Branch, Enugu

22. Okpara Avenue Branch, Enugu

23. Enugu Road Branch, Nsukka

FIRST BANK OF NIGERIA PLC

24. 9th Mile Corner Branch, Ngwo-Enugu

25. Ehalumona Branch, Nsukka

26. Emene industrial Estate branch, Enugu

27. 35 Ogui Road Branch, Enugu

28. 21 Okpara Avenue Branch, Enugu

29. New Haven Branch, Enugu

30. Uwani Branch, Enugu

31. Ikem Branch, Via Nsukka

32. Inyi Branch, Oji River

33. Enugu Road Branch, Nsukka

34. UNN Branch. Nsukka

35. Obollo Afor Branch, Nsukka

36. Orba Branch, Nsukka

37. Ovoko Branch, Nsukka

FIRST CITY MONUMENT BANK PLC

38. 41 Garden Avenue Branch, Enugu

39. 12A Market Road Branch, Enugu

FIRST INLAND BANK PLC

40. Agbani Branch, Enugu

41. Okpara Avenue Branch, Enugu

42. University Road Branch, Nsukka

GUARANTY TRUST BANK PLC

43. Ogui Road Branch, Enugu

44. Rangers Avenue Branch, Enugu

45. University Road Branch, Nsukka

INTERCONTINENTAL BANK PLC

46. ESUT Branch, Agbani-Enugu

47. Kenyatta Branch, Enugu

48. Ogui Road Branch, Enugu

49. Okpara Avenue Branch, Enugu

50. Enugu Road Branch, Nsukka

51. Orba Road Branch, Nsukka

52. UNN Branch, Nsukka

OCEANIC BANK PLC

53. Ogui Road Branch, Enugu

54. Agbani Road Branch, Enugu

55. Garden Avenue Branch, Enugu

56. Emene Branch, Enugu

57. University Road Branch, Nsukka

58. Obollo Afor Branch, Nsukka

SKYE BANK PLC

59. Ogui Road Branch, Enugu

SPRING BANK PLC

60. 9 Ogui Road Branch, Enugu

61. 138 Ogui Road Branch, Enugu

62. 58 Ogui Road Branch, Enugu

STANBIC IBTC BANK PLC

63. Ebeano Housing Estate Branch, Enugu

STERLING BANK PLC

64. 2 Ogui Road Branch, Enugu

UNION BANK OF NIGERIA PLC

65. Agbani Branch, Enugu

66. Emene **B**ranch, Enugu

67. Ogbede Branch, Igbo-Etiti LGA

68. Ogui Road Branch, Enugu

69. Garden Avenue Branch, Enugu

70. 9th Mile corner Branch, Ngwo-Enugu

71. Ogbete Main Market Branch, Enugu

72. Okpara Avenue Branch I, Enugu

73. Okpara Avenue Branch II, Enugu

UNITED BANK OF AFRICA PLC

74. Agbani Road branch, Enugu

75. Aguobuowa Branch, Ezeagu LGA

76. Aji Branch, Enugu-Ezike, Nsukka

77. Okpara Avenue Branch I, Enugu

78. Okpara Avenue Branch II, Enugu

79. Ebeano Pocket Estate Branch, Enugu

80. Kenyatta Branch, Enugu

81. Enugu Main Branch, Enugu

82. 9th Mile Corner Branch, Ngwo-Enugu

83. PPMC Complex, Emene Branch, Enugu

84. Umulokpa Branch, Uzouwani LGA

85. UNEC Branch, Enugu

86. UNTH Branch, Enugu

87. Ogbete Main Market Branch, Enugu

88. Trans Ekulu Branch, Enugu

89. UNN Branch, Nsukka

WEMA BANK PLC

90 Ogui Road Branch, Enugu

ZENITH BANK PLC

91. 0kpara Avenue Branch, Enugu

92. Ebeano Estate Branch, Enugu

93. Trans Ekulu Branch, Enugu

94. Presidential Road Branch, Enugu

95. Zik Avenue Branch, Enugu

96. Enugu Road branch, Nsukka

Source: Central Bank of Nigeria (CBN), October 2008.