

Nigerian Journal of Management Technology & Development



*A bi-annual Publication of
School of Management Technology
Abubakar Tafawa-Balewa University, PMB 0248, Bauchi-Nigeria*

JOMATECH

ARTICLES IN THIS ISSUE

A Review of the Contributions of the Stock Exchange to the Nigerian Economy (1986-2005) <i>Aminu Kado Kurfi, PhD</i> - - - - -	I
Regulation in Nigerian Telecommunication Industry: Perception of Mobile Phone Providers: <i>Aminu Ahmad & Bello Usman Jada</i> - - - - -	10
Import-Export Demand Functions and Balance of Payments Stability in Nigeria: A Co-integration and Error Correction Modeling: <i>Shehu Usman Rano Aliyu PhD</i> - - - - -	18
Bank Recapitalization and Implications for the Nigerian Economy: <i>Aliyu Mamman PhD</i> - - - - -	35
Information and Communication Technology, a Tool for Fraud Prevention and Detection in the Banking Industry: <i>Pantami, I, A, I. & Arabi A, A</i> - - - - -	45
Comparative Analysis of the Distribution of Manpower According to States of Origin in the Federal Civil Service: 2000 & 2004: <i>U G Moti, PhD and C J Mbah</i> , - - - - -	48
Empirical Test of the Relationship between Growth in Bank Capital Base and Profitability: A Case of FBN and UB Plc) <i>James. O. Alabede</i> - - - - -	57
Fiscal Transparency in Nigeria: an Evaluation of the Checks and Balances in the Constitution of the Federal Republic of Nigeria 1999 : <i>S. S. Maimako, PhD</i> - - - - -	63
Analysis of Influence of Sales Promotion Type on Micro-Business Enterprises' Sales Volume in Gombe Metropolis: <i>Knights, E.D and Jo Gold Aliboh</i> -- - - -	74
Lagrangian Interpolation Polynomial Approximation of Demand Curve Based on the Sales of Tomatoes in Bauchi Metropolis, Nigeria: <i>Adamu, M. M., Garba, E. J. D., Hamidu, B. M</i> - - - - -	78
An Empirical Analysis of Customers' Perception of Electronic Banking in Nigeria: <i>John Itodo</i> - - - - -	83
Measuring the Impact of Innovation on Firm Value: An Empirical Approach : <i>E.O. Oni</i> - - - - -	93
Currency Management in Nigerian: A Way Forward: <i>Umar Usman, and Ldama John</i> - - - - -	102
Polynomial Approximation of Demand Curve Based on the Sales of Onions in Bauchi Metropolis, Nigeria: <i>Adamu, M. M., Garba, E. J. D, Hamidu, B. M</i> - - - - -	108
An Analysis of World Bank Procurement Strategies in Project Implementation: A Study of Selected Projects in Adamawa State: <i>Haruna Isa Mohammeda and Kwaji Duguri</i> - - - - -	113
Consumer Purchase Preferences of House Wives in Government Residential Areas in Maiduguri: <i>Bananda Robinson</i> - - - - -	123

Information and Communication Technology, a Tool for Fraud Prevention and Detection in the Banking Industry

Pantami, I, A, I.

Management and Information Technology Programme* isapantami@yahoo.com +234-803-426-4909
&

Arabi A, A

Accounting Programme, School of Management Technology, Abubakar Tafawa Balewa University Bauchi, Nigeria

Abstract

The pervasiveness of fraud and forgeries in the banking industry is a cause for concern for the economy. Millions of Naira is lost due to fraudulent practices. As such it is the objective of this research to investigate the prevention and detection of fraud in the banking industry using information and communications technology. The methodology used is the survey research method that used a structured questionnaire. Three sample banks were drawn through systematic sampling from a total population of 19 banks operating in Bauchi metropolis. Descriptive statistics and analysis of variance (ANOVA) were the methods of data analysis. It is found that information and communications technology as well as internal control mechanism help in fraud prevention and detection. The study concludes with the following recommendations: the need for the development of appropriate software, good recruitment and compensation system, constant periodic check and job rotation in the banking industry.

1.0 Introduction

A high percentage of fraud and forgery cases in the banking industry have been observed to be perpetrated by or in conjunction with staff members. Indeed it is noted that most big banks fraud that succeeded have internal collaborators. Nigerian Deposit Insurance Corporation statistics on banks staff involved in fraud and forgeries shows that cooperation staff such as supervisors, officers, accountants, managers, executive assistance, clerks and cashiers accounted for about 90.6% of the total bank fraud attributable to staff (Isiaka, 2004:3).

Fraud is an action, which involves the use of deceit and tricks to alter the truth so as to deprive a person of something which belongs to him or something to which he might be entitled. The intention of the fraudster is to dishonestly benefit himself to the detriment of a legitimate beneficiary of such property or right (Nasir, 2006:2, Adebayo, 2005, Smith, 1999, Encarta premium, 2004). One thing that characterizes fraud and makes it different from other

crimes is that the application of physical force, violence or threats may not be involved to carry it out (Smith 1999).

Between March and May, 2004 available statistics showed that no fewer than 82 bank workers lost their jobs for direct involvement/or complexities in fraud cases, totalling N921 million of which N431.9million was successful (This day, 2004:29). The level of fraud is of great concern to all stakeholders, i.e. shareholders, customers, staff, regulators, government, consultants e.t.c. because the banking industry is one pivotal industry in which any economy rotates and because new fraudulent schemes are continually surfacing, just as quickly as one type of fraud is detected another is introduced hence, the number of reported cases of fraud has continued to increase over the past years. It is estimated that averagely, banks lose about 6% of annual revenues to fraud and about N1700 per day per employee to fraud. Data available from the 2003 annual report of

the Nigerian Deposit Insurance Corporation (NDIC) showed that the reported cases of fraud increased from 182 in 1999 to 908 in 2003. The total amount involved was N6,367,690 for 1999, N2,851,110 for 2000, N11,243,940 for 2001, N12,919,000 for 2002 and N9,383,000 for 2003.

With the world being a global village now because of globalisation, this resulted in high competition by organisations to meet up with the challenges of embracing information and communications technology for efficient management of their operations. Since the whole world is now becoming information technology compliant, therefore, fraud control is not complete without looking at how information and communications technology can be used to prevent and detect it.

2.0 Methodology

The research is a survey where the accurate assessment of the characteristics of registered banks and staff were studied. The population of the study consisted of all the branches of the registered banks operating in Bauchi metropolis. However, it was not feasible to study the whole population and therefore sampling method was inevitable. The research thus employed systematic random sampling. The systematic random sampling was used to choose the number of banks. Data collected through questionnaire were presented in tabular form and analysed by a simple descriptive statistic and the hypothesis will be tested through Analysis of Variance (ANOVA).

3.0 Data Presentation, Analysis and Interpretation

The management of data and information is a major challenge to organizations of all kinds, and to individuals within organizations. Data need to be summarized and presented so that people, not

computers can understand what is happening. The data collected from the respondents of the selected banks were analyzed by the use of tables and simple percentages calculated to ascertain the degree of responses made by the respondents, which formed the basis for the acceptance or rejection of the hypothesis postulated in the research.

A total of 87 questionnaires were administered to the respondents all of which were duly completed and returned. The presentation was therefore, based on the responses of the 87 respondents.

Table 1: Department of Respondents

Variable	Frequency	Percentage
Internal Audit	25	28.74
Credit Control	28	32.18
Banking Operation	20	22.99
Marketing Department	10	11.49
Others	4	4.60
TOTAL	87	100

Table 2: Qualification of Respondents

Variable	Frequency	Percentage
GCE/SSCE	-	-
OND/NCE	33	37.93
HND/BSC	30	34.48
MBA/MSC	24	27.59
TOTAL	87	100

Table 3: Awareness of Fraud

Variable	Frequency	Percentage
Yes	87	100
No	-	-
TOTAL	87	100

Table 4: Sources of Information about Bank Fraud

Variable	Frequency	Percentage
Employee Handbook	50	57.35
Induction Course	87	100
Notice Board	12	13.79
TOTAL	149	100

Table 5: Nature of Bank Frauds

Variable	Respondents	Percentage
Internal/employee fraud	30	34.48
External fraud/customers	27	31.04
Mixed fraud	30	34.48
Total	165	100

Table 6: Persons involved in frauds and forgeries

Variable	Frequency	Percentage
Top management	17	19.54
Customers	09	10.34
System analyst	21	24.14
Tellers/cashiers	33	37.93
Others	07	8.05
Total	87	100

Table 7: Internal control and fraud detection

Variable	Frequency	Percentage
Yes	63	72.41
No	24	27.59
TOTAL	87	100

Table 8: How does internal audit control fraud in your Bank

Variable	Frequency	Percentage
Enforcing compliance	17	19.54
Monitoring of systems	09	10.34
Review of customer activities	21	24.14
Periodic auditing	33	37.93
Total	87	100

Table 9: Detection of fraud

Response	Frequency	percentage
Whistle blowing	14	16.09
Customer complaint	16	18.39
Reconciliation of account	29	33.33
Stock-taking	20	22.99
Changes in life styles of culprit	08	09.20
Total	87	100

Table I0: Effectiveness of information and communications technology in fraud prevention and detection

Response	Respondents	Percentage
Yes	87	100
No	00	00
TOTAL	87	100

The entire respondent (100%) agreed that ICT is a veritable tool in effective fraud prevention and detection.

Table II: Fraudulent Practices

Response	Respondents	Percentage
Password cracking	43	49.43
Scavenging	22	25.29
Piggybacking	15	17.24
Terminal spoofing	07	08.04
TOTAL	87	100

Source: Questionnaire administered, 2007

The presentation was based on the responses of 87 respondents. In terms of departments, 25 were found to be in internal audit (28.74%), 28 in credit control (32.18%) and 34 in Banking operation (22.99%), marketing (11.49%) and others (4.60%) Regarding qualification of respondents, 33 (37.93%) are OND/NCE holders 30 (34.48%) HND/BSC holders and 24 (27.59%) have MBA/MSC qualification.

All 87 (100%) of the respondents were aware of fraudulent practice in their respective organization in which 50 (33.56%) were aware of it (fraud) through employee handbook, 87 (58.39%) through induction course and 12 (08.05%) through notice board. Internal employee fraud in the banking industry is far-reaching 34.48%, the external fraud represent 31.04% of the response. All the respondents pointed out that both internal and external fraud are widespread in the banking industry. Looking at the category of persons involved in fraud and forgeries in the banks, tellers and cashiers were rated highest with 37.93%, the system analyst or information technology staff were second with 24.14%, top

managers accounted for 19.54% and customers 10.34%.

72.41% respondents pointed that internal control mechanism is an effective method in the prevention and detection of fraud. Reconciliation of account and stock taking (33.33%) and 22.99% are the major ways of detecting fraud. All the respondents (100%) agreed that information and communication technology is a veritable tool in effective fraud prevention and detection. Concerning fraudulent practices, 49.43% of the total respondents were of the view that password cracking is the most prevalent fraudulent practice in the banking sector while 25.29% were of the view that scavenging is the most prevalent. Piggybacking was 17.24% and terminal spoofing was 8.04%.

37 of the respondent strongly agreed that all staff using information technology facilities have password, 39 agreed, 3 undecided, 5 disagreed and 3 strongly disagreed. 27 of the respondents disagree that staff passwords are frequently changed by system analyst and 25 strongly disagreed. Regarding staff access to the central computer systems, 40 of the respondent strongly disagreed that all staff in the organization have access to the central computer system. 33 of the respondent agreed that information technology system in the organization have attribute identification devices.

54 of the respondents strongly agreed that all entries by computer operators are rechecked to detect errors. 66 of the respondents are of the view that information and communication technology facilitates efficient and correct service delivery to customers by eliminating delays, while 10 are undecided, 15 disagreed. 56 of the respondent

ber 2007
ng. The
selected
d simple
agree of
med the
pothesis
ed to the
eted and
ased on

percentage
3.74
2.18
2.99
1.49
60
30
percentage
7.93
4.48
7.59
30
percentage
00
00
percentage
3.56
8.39
8.05
00
percentage
14.48
11.04
14.48
100
percentage
19.54
10.34
24.14
37.93
28.05
100
percentage
72.41
27.59
100
percentage
19.54
10.34
24.14
37.93
100

strongly agreed that network failure have been the major obstacles in efficient service delivery and committing of fraud. 60 of the respondents strongly agreed that the use of information and communication technology has drastically reduced the incidence of fraudulent practices in the organization.

4.0 Testing Hypotheses:

A statistical test of a hypothesis can be likened to a court trial. The test of hypothesis ends up in either accepting the null hypothesis or rejecting the alternate one and vice versa. Two hypotheses were formulated in this project. They are:

a. Ho: Efficient and effective internal control does not minimise the occurrence of fraud in the banking industry;

HI: Efficient and effective internal control minimises the occurrence of fraud in the banking industry.

b. Ho: ICT will not ensure efficient and effective fraud prevention and detection.

HI: ICT will ensure efficient and effective fraud prevention and detection.

4.1 Testing hypothesis (a)

The examination of this hypothesis has been answered by the information on tables 7, 8 and 9. Supportive answers were provided by tables 3 – 6. On table 7, 72.41 percent of the respondents believed that internal audit is effective in the prevention and detection of fraud. This control is usually affected through periodic auditing (37.93%); review of customer activities (24.14%); enforcing compliance (19.54%); and monitoring of systems (10.34%). Internal audit becomes necessary because internal/employee fraud constituted

34.48% of all the fraud committed in b table 5). The people perpetrating the inter are members of top management (customers (10.34%); system analyst (24.1 tellers/cashiers (37.93%). The frauds com these persons are detected through: reconc account (33.33%); stock-taking (22.99); complaint (18.39); whistle blowing (16 changes in life style of culprits (9.2%). this analysis, it can be deduced that hypothesis (H0) is rejected and the hypothesis (HI) is accepted. Therefore it concluded that: efficient and effective control minimises the occurrence of fra banking industry.

4.2 Testing hypothesis (b)

The analysis of this hypothesis has been an the information on table IO, II, and I2. IO, 100% of the respondent repl information and communication techr relevant in fraud prevention and detection. frequently practiced form of fraud is cracking with 49.43%; scavenging piggybacking (17.24%) and terminal (8.04%). The five point Linkert-scale w analyze the responses by way of analysis o The condition here is that high mean coefficient of variance is acceptable. But mean is low and the coefficient of varian there is a problem with the response. require strategic decisions to correct the we

Table 12: Mean – Coefficient of Variance.

Variable	Mean	St.D.	V	C.V.
All staff using information technology facilities have password	4.17	1.33	0.17	0.32
Staff passwords are frequently changed by the system analyst	2.61	1.45	2.10	0.56
All staff in the organization have access to the central computer systems in the organization	1.76	0.83	0.67	0.47
All the information technology systems in the organization have attribute identification devices.	3.67	1.29	1.67	0.35
All entries by computer operators are re-checked to detect errors.	4.20	1.35	1.83	0.32
Information technology facilitates efficient and correct service delivery to customers by eliminating delays.	3.98	1.30	1.70	0.33
Network failures have been the major obstacles in efficient service delivery and committing of fraud	4.55	0.66	0.44	0.15
The use of information technology has drastically reduced incidence of fraudulent practices in the organization	4.67	0.81	0.66	0.17

Source: Questionnaire administered, 2007

It could be seen from the table above that rows 1, 4, 5, 6, 7, and 8 shows favourable mean (3.00 – 4.99) and low coefficient of variance of (0.15 -0.35). This indicates that the variable defining the efficiency of ICT is favourable.

The variables requiring serious management attentions are row 2 and 3, with low mean and high coefficient of variance. Therefore in line with the data presented in table 10, 11, and 12, the researcher concluded that the null hypothesis is rejected and the alternate hypothesis which states "ICT will ensure efficient and effective fraud prevention and detection" is accepted.

5.0 Conclusion

Though it is recognized that information and communications technology would certainly cost a lot of capital to deploy, it would be a wise investment decision strategy for banks to do. Computers and telecommunication systems have become very important as delivery systems and productive tools of electronic data

and information. Nigerian financial institutions have now realized that financial services today require prompt prevention and detection of fraud, delivery of services, efficiency and the ability of customers to be served in any of the branches in any part of the country, without any impediment. As a result of these, financial institutions are embarking on the use of computer applications software that can help to provide efficient, comprehensive and nationwide services to their customers, and these have resulted in an overwhelming customers-satisfaction. It can therefore be concluded that the prevention, control and detection of fraud rest squarely on the ability of the management of any organization to implement internal control mechanisms through the use of information technology.

6.0 References:

- Adewunmi, W. (1992): Bank Audit UNILAG Press, Lagos
- Alvin, A. & James, W. (1991): Auditing an Integrated Approach, 5th Edition. Prentice-Hall International USA
- Bank and Other Financial Institution Act (BOFIA) (1999)
- Brochow, J. M. (1997): Information Overload – Creating Value with New Information Systems Technology, Prentice Hall Inc., London.
- Buckholz, T. J. (1995): Information Proficiency – Your Key to the Information Age, International Thomson Publishing Inc, New York.
- Bysinger, B. and Ken K. (1996): Investing in Information Technology, International Thomson Publishing Inc, New York.
- Company and Allied Matters Act, 1990
- Cortada, J. W. (1998): Best Practices in Information Technology, Prentice Hall Inc, New Jersey.
- Dandago, K. I. (1990): Auditing in Nigeria: A Comprehensive Text, Adamu Joji Publishers, Kano, Nigeria.
- Encarta ® Premium Suite, (2004) <http://www>.
- Galliters R. D. & Walter, B. (1998) Information Technology and Organizational Transportation: Innovation for the 21st Century Organization, John Wiley & Sons, Chicester.
- Helen, J. (2006): Fraud Detection and Control in Nigerian Banks, International Journal of Accounting vol. 2 No. 3, pp. 12 – 17.
- Huang, K. et al (1999) Quality and Information Knowledge, Prentice Hall Inc. New Jersey.
- International Auditing Guidelines (IAG 6)
- Isiaka, U. I. (2004): "Fraud Control through Ethics and Professionalism" Being a paper presented at the Compulsory Continuing Professional Development Programme (CCPD) of the Chartered Institute of Bankers of Nigeria – Lagos Airport Hotel Ikeja, Tuesday, November 30, 2004.
- Kalakota, R. & Fret, F. X. (1996) : Frontier of On-Line Financial Services, Working Paper, University of Rochester, New York.
- Kennedy, A. J. (2004): A Rough Guide to the Internet, Rough Guide Limited, London
- Liebowitz, J. (2000): Building Organizational Intelligence – A Knowledge Management Primer CRC Press, Boca Raton.
- Luftman, J. N. (1996) Competing in the Information Age – Strategic Alignment in Practice, Oxford University Press, New York.
- NDIC Annual Report and Accounts, 1990-2003.
- Nicholas, R. (2000): Defending Your Digital Assets against Hackers, Crackers, Pies and Thieves, McGraw Hill, California, USA.
- Nwoko, C. (1988): Internal Control in Business ABIC Book and Equipment Ltd. Enugu, Nigeria.
- Smith, G. R. (1999): "Best practice in fraud prevention" Being a paper presented at the National Outlook Symposium on Crime in Australia convened by the Australian Institute of Criminology held on Canberra 22-23 March 1999.
- Sprague, R. H. (1990): Information Systems Management in Practice, Englewood Cliffs, N. Prentice-Hall.

Sveiby, E. K. (1997) *The Organizational Wealth – Managing and Measuring Knowledge-based Assets*, Berrett-Koehler Publishers Inc, San Fransisco.

Weber, Ron (1999): *Information Systems control and Audit*, Prentice Hall, USA.

Woods, I. (1998): "Fraud and the Australian Banking Industry" A paper presented at the Conference Crime

against Business. Covered by the Australian Institute of Criminology, Melbourne 18 – 19, June 1998.

Woodall, J. et al (1997) *Total Quality in Information Systems and Technology* St Lucie Press, Florida.

Woolf, E. (1986): *Auditing Today*. London, Prentice-Hall International Inc.

of On

ersity of

e

izational

Printer

ormation

Oxford

003.

al Asset

McGraw

Business

eria.

in frau

the 3

Austral

ninolog

System

fs, N.