



AN EXPLORATORY APPROACH ON CALL-OVER SYSTEM: A CONTINUOUS AUDIT TECHNIQUE FOR FRAUD DETECTION AND PREVENTION IN BANKING SECTOR

Hussaini Mukhtar¹, Arafat Ahmad Hussain² and Aisha Umar Asheikh³

^{1,2,3}Accounting Department Faculty of Social and Management Science, Borno State University

Abstract

Recent development in financial technology has expedited the work and veracity of internal audit in banking sector. Call-over emerged as a continuous auditing mechanism and leverage this technology to incessantly monitor and examine large amount of banking transactions in real-time in part to prevent/detect fraud at the same time providing assurance on the effectiveness of the internal control of the bank. The objective of this paper was to examine the impact of call-over on detection and prevention of fraud in banking sector and to illustrate the practical application of Call-over in banking sector. The paper uses filtering technique to select 12 banks which form the sample size of the study. Genuine banking transactions were collected at random as a case study to detect fraud risk. Call-over was then applied to these transactions using Extensive Business Reporting language (XBRL) to identify irregular transactions. Findings reveal four suspicious transactions with irregular processing. We conclude that call-over has a significant impact on fraud detection and prevention in banking sector and that fraud potential is more ubiquitous in cash and tellering than customer service, fund-transfer or any other department in deposit money banks. We recommend that internal audit of banks be strengthen in order to support the bank's anti-fraud management efforts necessary to protect the bank. We further recommend that staff be mandated to call-over the transactions of their fellow colleagues on a daily basis and the result thereof be reported the branch internal auditor.

Keywords

Call-over
Continuous auditing
Financial Technology
Internal control
Telling

JEL Classification

Corresponding author

Arafat Ahmad Hussain
elhussaeny@gmail.com
Phone NO: 07031202677



1. Introduction

With the growing demand for Information Technology and the increased transaction volume in the banking sector, users of accounting information require record to be timely, relevant and reliable. These requirements consequently necessitate the need for continuous audit, a system of non-stop monitoring of transactions. Data collected from annual report

of eight deposit money banks in Nigeria for the year 2020 showed a loss of ₦1.9bn as a result of fraudulent activities (Amarachi, 2021). Information technology has dramatically expedited the incidence of fraud in banking sector. In this sense, auditors and professional accountants in Management Information System (MIS) sought to find a way to mitigate these risks in order to give banks the confidence to collect

deposits and process customer transaction. Call-over allows for instantaneous examination of transactions through a robust combing of high-volume data electronically. Consequently, the call-over mechanism shows itself to be a reliable technique in fraud detection and prevention.

One of the primary functions of an auditor during an audit exercise is to verify the quality of the data (Fernando et al., 2008). A measure of data quality is the number of errors within a database because virtually all banking services in Nigeria are offered using accounting software. Data from these softwares are kept in a secure server, this ranges from human resources data, accounting data, finance and procedural information. All records kept in the banks' database have the characteristics of important inputs in organizing the business processes of the related departments. Therefore, it can be said that there are internal audit activities among the areas where these data sets can be used most effectively (İsmail, 2019). The accounting and procedural data are robustly used by internal auditors to perform Call-over on historically processed and immediately consummated transactions and report to management continuously under the guide of Computer Assisted Audit Techniques (CAATs). With transaction call-over, audit risk can be controlled to a higher degree since there is no need to sample transactions, the margin of error is minimized to its minutest chance. The internal auditor can subject all transactions to a forceful compliance test notwithstanding the volume of the transactions. This is mostly pragmatic in the banking sector since all transactions processed are called over on a daily basis to check for accurate postings and possible errors.

In this respect, call-over as a continuous audit approach plays a vital role in immediate detection and prevention of fraud in the banking sector. The process of detecting and controlling fraud using call-over is presented as a case study in this paper.

2. Problem Statement

In an ever increasing complex business environment, banking sector like no other remain the most susceptible sector exposed to the risk of fraud because of its fundamental nature of dealing with physical cash and electronic fund, hence the need for developing mechanisms for fraud detection and prevention became of paramount importance. The sector is at the forefront of financial innovation to harbor its complex dealings and its large volume of data generated on a daily basis from transactions with individual and corporate customers. This calls for the need to critically analyze this large chunk of data and transform them into useful information partly to detect suspicious transactions that are risky and in part to prevent fraud (from happening) that might result into loss of fund or reputation in future. Call-over emerged as the most efficient continuous audit technique used by Nigerian banks in converting data into meaningful information to speed up the time it'd take to detect risky transactions as they occur. However, very little or nary is found on call-over in the literature. Despite the efficiency of call-over, huge amount of fraud are reported yearly by banks in Nigeria. This raises a question of professional skepticism: Is the call-over system truly effective? This among other questions is what this paper intends to answer, hence the objectives of the study are to:

- i. Examine the impact of Call-over on fraud detection and prevention in Nigerian banking sector.
- ii. Illustrate the pragmatic application of call-over in detecting fraud amidst a large pool of transactions.

3. Call-Over

Call-over is a system of continual examination of posted transactions to test for compliance and possible errors or fraud. It is both a relational and network Database Management System (DBMS) used by banks to store information relating to transaction history. The internal

auditor rigorously scrutinizes these transaction electronically and compare each posted transaction with its supporting document (instrument: cheque, deposit certificate, voucher, etc.) to check for compatibility of the posting with the instructions on the instrument and accuracy of transaction processing. Test is then run on the transactions as a whole to check for proper balancing of cash and cash equivalent.

Call-over mechanism take advantage of Information Technology and scrutinize transactions that are outside the procedural configurations in which a customer would normally follow to transact in an ordinary customer bank relationship. These transactions are called “exception” and are immediately identified without delay. Where disparity is found in isolated transactions between what was processed on system and what is on the instrument, the transaction is saved as ‘exception’ and called over for audit enquiry, hence the term call-over. Given that this process is performed daily or in real time, call-over allow auditors to verify immediate transactions and continually test historical transactions for fraud and likely errors. In this sense, continuous auditing allows banks to produce audited financial statements immediately as demanded (evergreen report).

The testing of internal control reliability is usually performed at the same time of transaction testing. The transactions are primarily tested to check whether erroneous or irregular processing has taken place. This continuous testing help to reduce the complexity of tests of balances which must be performed at the date of statement of financial position. Tests performed on balances are generally done to gather audit evidence, on which the auditor ground his/her opinion on the true and fair representation of financial statements.

3.1 Continuous Audit

The primary purpose of an Auditor is to express his/her opinion on subject matter for which

management is responsible. In order to do this, the auditor is faced with the task of validating the accuracy of financial data and the reliability of the database which process, transport, and store these transactions. Assessing the data for accuracy entails checking for fraud and error in transactions. There are well established CAATs that are commonly used in search for material misstatements in financial records. Using these technologies within a continuous auditing system extend their effectiveness, as all transactions are analyzed in real-time.

In this sense, continuous auditing become commonly associated with three models each of which has a somewhat relative view of what CA is and how it works. The models differ slightly to some extent even though they are all built on the same conceptual framework. The most widely accepted definition of CA is the one published in 1999 by AICPA which states that “Continuous auditing is a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors’ reports issued simultaneously with, or a short time after, the occurrence of events underlying the subject matter (CICA/AICPA, 1999). Rezaee, et al. (2001) define CA in their model as a process of gathering and evaluating evidence to determine the efficiency and effectiveness of real-time accounting systems in safeguarding assets, maintaining data integrity, and producing reliable financial information. In this model, data are collected from transactional systems by linking tables, via storage drives, File Transfer Protocol (FTP) or via external network servers. Data are then extracted from a variety of platforms and systems and transformed by validating, cleaning, restructuring the data and “scrubbing” with business rules. Finally, standardized tests are run within the data mart continuously or at predetermined intervals to gather audit evidence and issue exception reports.

Woodroof and Searcy’s (2001) model discussed the concept of CA in relation to debt

covenant compliance. Their model makes use of web-based technologies. It draws attention to the need for a reliable and secure system. The model underscores conscientiously on the need for timely reports. This is referred in the model as evergreen report. The model has some weakness as the use of audit web technologies instead of application software may give rise to the susceptibility and vulnerability of the system to social engineering. Onions (2003) put forward a keystroke level data examination in his model. The model involves monitoring database utilities and applications for commands which could result to an error or fraud. The model addresses the testing of transactions in two ways, the first

of which state that each transaction must be audited and reported on as an isolated entity ephemerally. And secondly the transactions are examined as a whole over a long period of time (usually years) to look for patterns in the transactions which may perhaps mean an error or fund embezzlement.

To meet the requirements of continuous auditing, all of the models must address both internal control testing and testing of transactions. A dual-pronged approach, where both the system (internal controls) and data (transactions) are tested, simultaneously is the ideal (Flowerday et al. 2006). A comparison of these models is presented below.

Table 1. Comparison of Three Continuous Auditing Models

Rezaee et al. (2002)	Real-Time	Information is collected and processed on real time basis.
	Reliability of Internal Control	CAATS are used.
	Accuracy Within Transactions	Standardized audit tests are built into the system which is used to run continual test.
	Reporting Method	Web-based CAATs is used to transmit data to auditors' terminal.
	Data Format	Data mart (Data warehouse XBRL).
Onions	Real-Time	Systems run in parallel with operational database in real-time.
	Reliability of Internal Control	DBMS utilities such as Audit logs, Password control, and Web services verify information tools are used.
	Accuracy Within Transactions	Transactions are checked using CAATs at the time of entry and later.
	Reporting Method	Graded alerts sent through Virtual private networks (VPNs) to audit department/OLSAC.
	Data Format	Data Marts (XCAL).

Woodroof and Searcy	Real-Time	Real-time processing is the aim for this model.
	Reliability of Internal Control	Adapt and apply SYSTRUST principles: Must be in the auditor-defined rules for the digital agents.
	Accuracy Within Transactions	Data are analyzed by devices integrated into the system and it is rule-based detection by digital agents.
	Reporting Method	Evergreen reports are produced on demand through a web interface using information pull approach.
	Data Format	Does not interface with legacy systems.

Source: Adapted from Flowerday, Blundell and Solms (2006)

Several continuous auditing models exist most of which are merely conceptual. The above three models are the most pragmatic ones since they are largely implemented in the banking sector and beyond. These models were all built on the framework of Varsarhelyi and Halper (1991) popularly known as Continuous Process Auditing System (CPAS), an approach of paperless real-time internal audit developed at AT&T Bell Laboratories in the early 1990s. Call-over system in its entirety originated its

core from CPAS model of Rezaee et al. of 2002 in respect of data format, reporting method, transaction overriding, memo-postings, testing of internal control and real-time processing. The Razaee et al. model of continuous auditing is illustrated below.

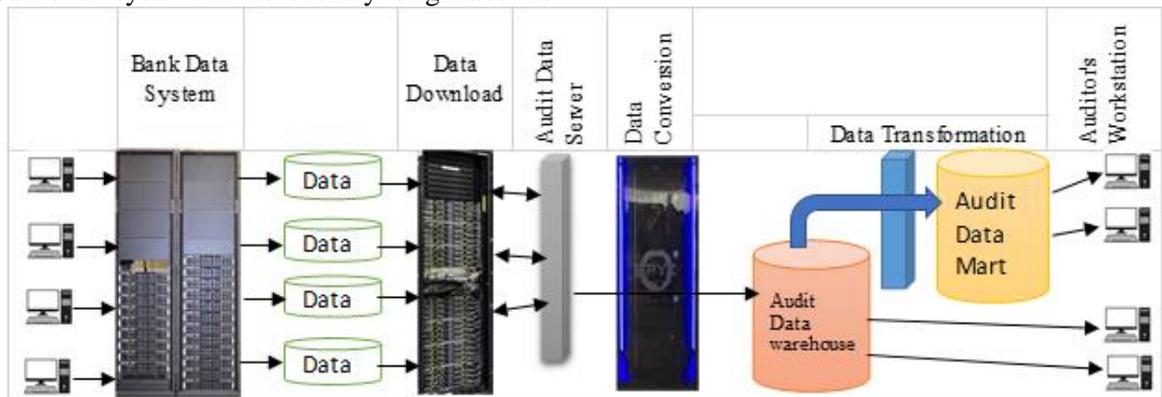


Figure 2. Continuous Audit Model
Adapted from Razaee et al., 2002

Transactions posted in Inter-switch, Real-Time Gross Settlement (RTGS), Reuters, and General Ledgers (GL) first hit the bank's mega data warehouse before dropping in the local branch server at the speed of light. These transactions will then be accessible for review or download by the internal auditors for their scrutiny. The internal auditors make sense of the data by subjecting them to call-over. All transactions (whether called over or not) are archived in the audit data warehouse. The internal auditors can at all-time access information (historical and concurrent) from their audit workstation through data retrieval function.

4. Literature Review

There is nary empirical literature on call-over in banks. In this context, some academic studies on internal audit practices based on continuous audit in banks are reviewed below.

Ismail (2019) studied central audit activities as a continuous audit approach in Turkish banking sector. The study uses some realistic banking transactions (though at random) as examples to examine the process related to savings account fraud in Turkey. This has been presented by providing basic information about the central audit activities applied as a continuous audit approach in the banking sector. Data mining technique (SQL) was then applied to these transactions to detect fraud risks. Four (4) fraud schemes with embezzlement indications were determined in 30,021 sequence of data. The study repeatedly emphasizes on the importance of data analytic technique as it saves time, cost and human resources at a very minute expense.

Fernando et.al (2008) in their study of Continuous auditing: a literature review, they adopt an exploratory approach to analyze the existing literature on CA. The study addresses the CA's concepts, models and implications using a total of 57 articles. The study reveals that out of the total papers selected, only one

represent an empirical research. Also, half of the non-empirical articles adopt a conceptual approach, mostly defining CA theories and models and presenting reasons and opportunities for its uses.

Rahman and Anwar (2014) studied the effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks. The study targeted the perception of Islamic banking employees therefore a survey method of a quantitative research technique was adopted to cross-examine 146 employee using questionnaire administered to bank managers and officers. Result of the survey reveal that protection software/application was seen as the most effective component of fraud prevention techniques.

Tang et al. (2017) study the use of data analytics in the internal audit function and assess the types of tools that internal auditors use for analytical purposes in fraud detection and control. The study adopted a qualitative research technique and uses interview to cross examine the population. Certified fraud examiners were interviewed and findings of the survey show that certified fraud examiners value data analytics. Result from the survey also show that they use data analytics techniques for different purposes and that a substantial amount of budget is allocated to the internal audit to support this function.

Bhambri (2011) studied the data mining applications in banking sector. The study was mainly theoretical. It explains the fraud detection procedure as a mechanism used in data mining processes. According to the paper, using data mining packages helps to identify the indicators that can lead to fund embezzlement. Similarly, Saran and Jayanthi (2015) explored and reviewed the data mining techniques in the banking sector in a theoretically based study. The study reveals that Banks who apply data mining techniques in their decision making substantially benefit and hold an edge over

others who don't. The study further reveals that banks use data mining in various application areas including but not limited to fraud detection, risk management, money laundering detection and investment banking. The study also reveals that banks use data mining techniques to forecast future events that can help in decision-making processes.

These researches show that Accounting data analytics applications in the field of fraud auditing have started to be used recently only in the past two decades and these techniques have made significant contributions in fraud detection and control. Therefore, it can be said that the management of accounting analytical techniques is crucial today in fighting against fraud in banking sector where a large volume transaction is performed.

5. Methodology

Data generated for the study was a result of one day (1st August 2022) transaction from twelve (12) different commercial banks in Nigeria. Filtering technique was used in selecting the sample of the study and the filters used were as follows:

Filter 1: The bank must be listed on the Nigerian Exchange Group (NGX) as at 1st August 2022

Filter 2: The bank must have its shares traded on the NGX as at 1st August 2022.

Filter 2: Data for call-over must be available and accessible from the bank for 1st August 2022.

The sample size after applying the above filters resulted in twelve (12) Nigerian banks made up of the following:

Table 1. Sample Size

Access Bank Plc.	First Bank of Nigeria	Union Bank of Nigeria Plc.
Stanbic IBTC Bank Plc.	Zenith Bank Plc.	Eco Bank Nigeria Plc.
Jaiz Bank Plc.	United Bank of Africa Plc.	Fidelity Bank Plc.
First City Monument Bank Plc.	Guarantee Trust Holding company Plc.	Unity Bank Plc.

Source: Field work 2022

A total of ten thousand (10,000) rows of data were collected which was used to create the database for the case study. The unusual transactions diverging from the internal control routine and procedures are considered as risk factors. These transactions are saved as 'exception'. The account numbers and General Ledgers (GLs) are all less than complete with

one digit, removed at random to ensure the privacy of the account holders and the banks.

The transaction reference codes are also entered with three digits less in order to eliminate the possibility of trace without authorization. Different banks have different internal policies and procedures but ultimately, they are all set to satisfy the Central Bank's guidelines. In this sense, all the twelve banks' internal procedures were synchronized with the Central Bank's guidelines so that harmony is established.

Table 2. Call-over Database: A Case Study

Poster's Class	Report Type	Posting Type		Retrieval Option	Posted Date	Action			
<input type="checkbox"/> Cashier <input type="checkbox"/> Non Cashier	<input type="checkbox"/> Called Over <input type="checkbox"/> Exception <input checked="" type="checkbox"/> Outstanding ✓	<input type="checkbox"/> Bulk <input type="checkbox"/> Single ✓		Poster: Identity Number	01/08/2022	Save Called over Save excepton			
Posted Transactions (Spooled)									
Effective Date	Account Number	Account Holder's Name	TC	Reference Number	Check No.	Debit	Credit	Posted Time	Sort by:
1/8/2022	001452456	Abba Garba Lawan	100	879935	-		350,000.00	8:12am	<input type="checkbox"/> Account No.
1/8/2022	601362428	Nacit B15	104	455737	32	50,000.00		8:24am	<input type="checkbox"/> Amount
1/8/2022	121230051	Mirovoy ventures	109	298467	11	190,000.00		8:32am	<input type="checkbox"/>
1/8/2022	121002300	Afsin Hessian	107	926363	11	-	190,000.00	8:32am	<input type="checkbox"/>
1/8/2022	00112	VAT Payable	201	648628	-		3.75	8:33am	<input type="checkbox"/> Search by Acct:
1/8/2022	00121	Service Fees	201	887662	-		50.00	8:33am	<input type="checkbox"/>
1/8/2022	601770051	Canan Enterprises	104	637653	233	250,000.00		8:58am	<input type="checkbox"/>
1/8/2022	001212457	Adamu Ali	100	926652	-		220,000.00	9:04am	<input type="checkbox"/>
1/8/2022	220099957	Andrew Francis	102	147826	-	200,000.00		9:07am	<input type="checkbox"/>
1/8/2022	001779455	Manager's Cheque	109	745726	149	700,000.00		9:12am	<input type="checkbox"/>
1/8/2022	00112	VAT Payable	201	745727	-		35.50	09:13am	<input type="checkbox"/>
1/8/2022	00112	Commision on M.C.	200	745728	-		300.00	09:13am	<input type="checkbox"/>
1/8/2022	001000457	Dankano Tours	107	745729	149		690,000.00	09:14am	<input type="checkbox"/>
1/8/2022	212004888	Chukwuma Paul	100	327030	-		210,000.00	11:00am	<input type="checkbox"/>
1/8/2022	602007814	Mary Buba Sani	100	428681	-		60,000.00	11:15am	<input type="checkbox"/>
1/8/2022	212671112	Blessing Ijabula	102	687257	-	15,500.00		11:22am	<input type="checkbox"/>
1/8/2022	224200552	Kaka Ali Abbas	102	234872	-	125,000.00		12:54pm	<input type="checkbox"/>
1/8/2022	601260001	MUM Enterprise	104	918763	1020	985,000.00		1:32pm	<input type="checkbox"/>
1/8/2022	000159133	Ebuka Abioudun	104	856121	215	40,000.00		1:42pm	<input type="checkbox"/>
1/8/2022	104222458	Adekunle Abiola	102	524715	-		115,000.00	1:56pm	<input type="checkbox"/>
1/8/2022	211987456	Stephanie Dominic	102	767682	-	25,000.00		2:32pm	<input type="checkbox"/>
1/8/2022	104031004	Kalli Muhammad Sabo	109	628592	88	550,000.00		2:12pm	<input type="checkbox"/>
1/8/2022	242463150	Abdullahi Idris	107	686721	88		550,000.00	2:27pm	<input type="checkbox"/>
1/8/2022	001197755	Bitrus Iliya	104	529789	21	33,450.00		2:36pm	<input type="checkbox"/>
1/8/2022	104641110	Tijjani Muhammad Cana	100	686211	-		225,000.00	3:00pm	<input type="checkbox"/>

Source: Field work 2022

All transactions are in Nigerian Naira (₦). The transactions are still outstanding, yet to be called-over as indicated by the report type in the third row, second column in Table 2 above. The transaction code (TC) is what determine if the account/GL is debited or credited, where 100, 107, 200 and 201 means credit to the related account and 102, 104 and 109 mean debit transaction to the related account/GL. Cash

lodgment is treated differently from cheque lodgment, the latter is knotted with two accounts both of which carry the same cheque number where one is debited (TC 109) and the other is credited (TC 107) with the same value. Transactions appear in the call-over immediately as they are posted. The internal auditor cross examines these transactions exclusively and issue report on the accuracy of all postings or

otherwise (where there are irregularities) to internal control on the findings of his/her examination. All the ten thousand rows were have been tested for compliance using Extensive

Business Reporting language (XBRL). The exceptions saved from the pool of transactions above is presented in Table 3

Table 3. Risk Factors Obtained from Call-over Test

Poster's Class	Report Type	Posting Type					Retrieval Option	Posted Date		Action
<input type="checkbox"/> Cashier	<input type="checkbox"/> Exception	<input type="checkbox"/> Single					Poster: Identity Number	01/08/2022		Saved exception
Posted Transactions (Spooled)										
Effective Date	Account Number	Account Holder's Name	TC	Reference Number	Check No.	Debit	Credit	Posted Time		
1/8/2022	001779455	Manager's Cheque	109	745726	149	700,000.00		9:12am		
1/8/2022	001000457	Dankano Tours	107	745729	149		690,000.00	09:14am	FALSE	
1/8/2022	108612678	Stephen Leonard	102	748923	-		115,000.00	1:56pm	FALSE	
1/8/2022	212381982	Musa Isa Umar	100	982374	54		30,000.00	11:22am	FALSE	
1/8/2022	124254511	Adamu Aliyu	100	564231		5,000.00		2:25pm	FALSE	

Source: Field work 2022

Transactions saved as exception usually calls for audit enquiry since explanation need to be given as to why the irregularities exist. Therefore, the scenario in figure 4 is commented with some exploratory query below. Judgment was exercised on the possible scenarios however for the reason that the instruments weren't available for physical examination.

Query 1

By virtue of cheque lodgment, transaction with reference number 745726 and 745729 on cheque number 149 are supposed to have the same value, but discrepancy exist.

Query! How'd the discrepancy came about?

Possible Scenario

In the potential fraudulent case above, it is reasonable to assume that the bank personnel suspiciously embezzled a sum of ₦10,000 since the receiving account should have gotten a total of ₦700,000 but then received ₦690,000 only.

Query 2

Customer withdrew money (judging by the Transaction Code "102" executed) on transaction with reference number 748923 and

value was credited to the account for the supposed transaction.

Query! Why was the customer credited instead of being debited?

Possible Scenario

In this case of this duplicitous transaction, cash was given to the customer and his account was also credited. This might have been an error on the site of the bank personnel or a devious mutual plan between the bank personnel and the customer to perpetrate ruse.

Query 3

Customer Musa Isa Umar deposited cash into his current account on August 1st, 2022. The value was credited but with a cheque number attached. Query! How did the cheque number came about?

Possible Scenario

This is most likely an erroneous processing by the cashier since no fraud possibilities could exist for such kind of scenarios. The cashier might have mistaken it for another entry and the value cancels each other accidentally.

Query 4

A customer deposited money into her account (judging by the Transaction Code “100”) and the account was debited with the original value of the cash.

Query! On what authority was the account debited?

Possible Scenario

In this suspicious case, the bank personnel accepted cash from the customer and erroneously or fraudulently debited the customer with the original value of the cash. This could be an obvious fraud attempt or a reckless mistake on the side of the bank cashier.

The records above must be examined in detail and further study their instruments to check for compatibility of the postings and the instructions. The existence of a possible error or fraud in these transactions must be established in the end. However, it is worth mentioning that all the anomalies detected in this call-over test have been identified and rectified by the internal auditors of the respective banks on the same day the transactions were processed since reversal of these transactions and their reposting were seen in the raw data generated.

6. Conclusion

The findings of this study reveal four suspicious transactions with fraud indication among high-volume data of 10,000 rows. Hence, it can be said that call-over is essential in detecting fraud risks in banks. In all the rows, the suspicious transactions were all items of cash and teller transactions, hence it is concluded that cash and teller unit has larger fraud risk than any other unit in any given deposit money bank in Nigeria. We conclude that call-over has a significant impact on detection and prevention of fraud in banking sector. The study recommends that internal audit of banks be strengthened in order to support the bank’s anti-fraud management efforts. However efficient the call-over is, it

would be hectic for one internal auditor to call-over all the transactions processed by all staff of a given bank branch on a daily basis, thence we recommend that staff be tasked with calling-over all the transactions of their fellow staff and reporting to the internal auditor.

References

- Amarachi, O. (2021). Fraud cases in Nigerian banks. <https://punchng.com/eight-banks-lose-n1-9bn-to-fraud-in-one-year/>
- Bhambri, V. (2011). Application of data mining in banking sector. *International Journal of Computer Science and Technology*. 2 (2), Pp 199-202.
- Charlton, G. & Marx B. (2009). An investigation into the impact of continuous auditing on the external auditors of the four largest banks in South Africa. <https://www.tandfonline.com/doi/abs/10.1080/10291954.2009.11435139>
- Central Bank of Nigeria (n.d.). List of CBN 419 Cases. <https://www.cbn.gov.ng/419/Cases.asp>.
- Fernando, D., Flávia C. D. S., & José A. B. (2008). Continuous Auditing: A Literature Review. *Organizações em contexto*. 4(7).
- Flowerday, S., Blundell, A. W. & Von S. R. (2006). Continuous auditing technologies and models: A discussion. *Computers & Security*. 25(1): 325–331 <https://www.doi:10.1016/j.cose.2006.06.04>.
- İsmail, K. (2019). Central audit activities as a continuous audit approach in the Turkish banking sector: a case study about frauds in savings accounts. *Marmara Üniversitesi Öneri Dergisi*. 15(53), 254-275. <https://www.DOI:10.14783/maruoneri.676406>.
- Onions R. L. (2003). Towards a paradigm for continuous auditing. <http://www.auditsoftware.net/community/how/run/tools/Towards%20a%20Paradigm%20for%20continuous%20Auditin1.doc>; [retrieved 1.04.2005].

- Rahman, R. A. & Anwar, I. S. K. (2014). Effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks. *Procedia-Social and Behavioral Sciences*. 145(1): 97-102.
- Rezaee, Z., Ahmad, S., Rick, E., & Peter, L. M. (2002). Continuous auditing: Building automated auditing capability. *Journal of Practice and Theory*. 21(1):147.
- Rezaee, Z., Elam R. & Sharbatoghlie A. (2001). Continuous auditing: the audit of the future. *Managerial auditing journal*. 16(3):58–150.
- Saran, R. S. & Jayanthi, S. (2015). A Review of Datamining applications in Banking. <https://DOI:10.4236/ce.2015.615165>.
- Tang, F., Norman, C. S. & Vandrzyk, V. P. (2017). Exploring perceptions of data analytics in the internal audit function. *Behaviour & Information Technology*. 36(11):1125-1136.
- The Canadian Institute of Chartered Accountants & American Institute of Certified Public Accountants (1999). Research Report: Continuous Auditing.
- Varsarhelyi M. A. and Halper F. B. (1991). The continuous auditing of online systems. *Auditing. A journal of practice and theory* 10(1):110–125.
- Woodroof, J. & Searcy, D. (2001). Continuous audit: mode development and implementation with a debt covenant compliance domain. *International Journal of Accounting Information Systems*. 2(1):91–169;