ISSN (Print): 2476-8316
ISSN (Online): 2635-3490
Dutse Journal of Pure and Applied Sciences (DUJOPAS), *Vol. 6 No. 3 September 2020*

Dark Side of IT Usage: Investigating Effectiveness of Information Security Controls Against Identity Theft Committed in Nigerian Banks

Musa Garba
Department of Computer Science
Kaduna State University
Email: musa.garba@kasu.edu.ng

Abstract
The dark side of Information Technology (IT) usage has been identified as a relatively new researchable area in the field of IT which covers the investigation of the negative consequences of IT use. Identity Theft is an example of such dark side of IT usage and it is used by fraudsters to criminally take control of customer or staff access rights in banks in order to defraud and annex for themselves funds which are not legally theirs. The three Nigerian banks used for this study will be represented as Bank A, B, and C. The objective is to understand the extent to which identity fraud affects Nigerian banks and what can be done to curtail the impact of huge losses suffered by the banks and their customers. Though banks are highly secretive industries because of their very sensitive customer data, responses were extracted from staff due to the existence of personal relationships. On analyzing the data, it is established that customer's inability to conform to controls/rules of the Banks, customers lack of awareness and non-proper implementation of controls by the banks as the chief reasons why we continue to have identity fraud theft in Nigerian banks. The study recommends that to ensure more control effectiveness against Identity fraud theft a thorough review and addition of system controls already on ground is thoroughly needed.

Keywords: IT Control, Dark Side of IT Usage, Identity Theft, Internal Control, Information Security

Introduction
The dark side of information technology is seen as a general name for a collection of negative results from information technology usage. These negative results consequently affect the wellbeing of people, organizations and/or establishments and the society at large. (Tarafdar, et al. 2015).

The term Identity theft refers to fraud that involves "pretending to be someone else in order to steal money or get other benefits". This proves to be an easy way of getting credentials of an unsuspecting person in order to defraud him. (Hedayati, 2014).

Identity theft has been classified as one of the fastest growing crimes in the world and one of the biggest contributors to terrorism, trafficking, money laundering, arms running etc. (Joel et al.2014). The intention of the fraudster is to make gains by using false identity, stolen identity, false identifications or stolen identity to defraud others. This enables gains such as monetary, goods and services or to avoid obligations. (Joel et al. 2014).

**Author for Correspondence*

"In Nigeria considering the sophistication and technical expertise invested in identity theft, it is safe to conclude that 90% of these attacks are financially motivated". (Monica, 2013).Huge losses are being recorded by both the banks and their customers due to identity theft daily. This work will unearth reasons why this persists while possible solutions will also be given. Banks are closed organizations as they vigorously resist giving out sensitive information especially information concerning their security and security incidents, hopefully this work will serve as a trailblazer where other researchers will take a cue to undertake more works especially on security issues as it relates to banks in Nigeria.

Problem Statement

The gap in this research comes from the following quote "With the dark side imperative, there is particular interest and scope for research in the area. In terms of societies and nations, future research could focus on potential outcomes in terms of information exclusion, disruptive patterns of work/living, Internet crime and pornography, identity theft and related issues, cyber-attacks and loss of privacy". (Tarafdar et al. 2015).

From the above gap Identity Theft has become a viable research area as stated in the above quote and thus necessary that researches be conducted on Identity theft fraud in Nigeria focusing on the banks that oversee maintenance of security controls despite their inaccessibility. Researchers need to find ways to circumvent that hindrance in order to proffer solutions to the raging problem of identity theft.

Tarafdar et al. (2015) has clearly identified identity theft as a viable research area which should be pursued. Banks in Nigeria have continued to suffer Identity theft for ages and researches need to be done to understand how deep this problem has eaten and what should be done to address it. By this study it is understood that identity theft fraud issues do exists in Nigerian banks with some of the problems identified and some solutions proffered.

Nigerian banks continue to groan under a lot of loses annually to fraudsters who employ the use of identity fraud to defraud their customers. Researchers find it difficult to approach banks for information regarding their operations because of their attitude of not giving out access to data to "outsiders" which could lead to compromise of customer information or organizational security. But then, this ugly trend of identity theft to defraud banks exists and is eroding the banks profit annually.

According to Nigerian electronic Fraud Forum (NeFF) Annual Report for2016released by the Central Bank of Nigeria (CBN), the banking industry recorded an astronomical increase of about 82% in reported fraud cases when compared to 2015 and over 1200% when compared to 2014. The 82% increase in the reported fraud cases amounted to an estimate of about NGN2.19 billion loss. Loss to identity theft played a good part in its realization.

In this light this paper will go beyond this age long banking shroud to bring out clearly the existence or otherwise of identity fraud in Nigerian banks. The paper will also underscore the main reasons why we have them and proffer some solutions to the menace. This research was made possible because the researcher haven also worked for many years in the bank in the IT audit department and has many colleagues in various banks and various departments who out of personal relationships provided the much needed in-road for the research to happen.

Due to the high incidence of identity theft cases in our Banks the aim of this study is to determine the effectiveness or otherwise of the security controls against identity theft in

Nigerian banks and come up with a framework that will ensure fewer occurrences. In this light the following important research question is formulated. How adequate and effective are the information security controls put in place by banks to safeguard customer deposits from identity theft fraud in Nigerian banks?

Research Approach

Different methods can be utilized in collecting empirical materials such as interviews, analysis of artifacts, documents, cultural record, direct observation, use of visual materials or personal experience. (Denzin and Lincoln, 1994, p. 14). Qualitative research involves the use of data from interviews, documents, and participant observation data, to understand and explain social phenomena. (Myers, 1997). The research question is best answered by a qualitative study as questionnaires; interviews and perusal of textual documents are involved in explaining the phenomena.

Questionnaires were distributed to Information Technology, Information Systems Audit, Internal Control and some experienced Operations staff with IT knowledge from three (3) banks in Nigeria marked here as Banks A, B and C. Responses were collected, analyzed, interpreted and presented as results.

Methodology

A qualitative methodology was adopted in order to get expert opinions from bank staff while some three (3) banks were chosen as case study. "Qualitative research involves the use of qualitative data, such as interviews, documents, and participant observation data, to understand and explain social phenomena". (Myers, 1997). An interpretive paradigm consisting of qualitative methods of data analysis which involves interviews, analysis of textual materials etc. was adopted in order to explain the phenomena under study.

The three banks used in this study are hereby represented as BANK A, B, and C. Case study researches are suitable for Information Systems research as we tend towards the study of information systems particularly in organizations especially since "interest has shifted to organizational rather than technical issues". (Benbasat et al., 1987).

Research Methods

"Interpretive studies generally attempt to understand phenomena through the meanings that people assign to them and interpretive methods of research in IS are aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context". (Walsham 1993, p. 4-5).

Questionnaires were used in order to sample opinions of various staff from different banks on various issues raised therein, analysis of textual material was also done on open ended questions raised in the questionnaire. A total of thirty-eight (38) bank staff responded to the questionnaires from the three (3) banks with ranks ranging from entry trainee (ET) to manager (Mgr.). The entire exercise took about three weeks.

Thirteen (13) staff responded from bank A with ten (10) male and three (3) female respondents. The age range of Bank A respondents is from 26 to 50 years and range of experience from one to twenty-one years. Eight of the respondents are core IT staff while remaining five (5) are Internal Control Division staff comprising Information Systems (IS)

Audit and internal control departments. There are eleven permanent staff and three contract staff. All the respondents have high computer literacy level.
There are Twelve (12) respondents from bank B comprising of eleven male and two females. Age range of respondents is from 26 to fifty (50) years with range of experience of four (4) to twenty-four (24) years. Nine (9) IT staff and three(3) internal control staff are the respondents with eleven (11) high computer literacy levels and one (1) mid-literacy level. Eleven (11) are permanent staff while one (1) is a contract staff.

Bank C has a total of thirteen respondents. Twelve (12) are male and one (1) female. Their age ranges are between twenty-five (25) and fifty (50) years with experience ranging from one (1) to twenty-five (25) years on the job. Nine (9) IT and four (4) internal control staff responded with nine (9) with high computer literacy level and four (4) with middle level computer literacy. The entire thirteen (13) respondents are permanent staff of the bank.

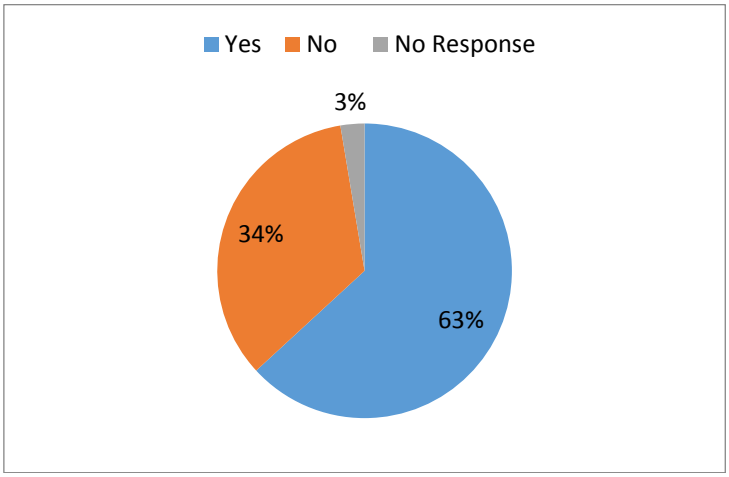
Results and Discussion
In answering the research question a questionnaire was prepared and shared to IT and Internal Control staff of 3 Nigerian banks A, B and C. First an attempt was made to find out if Identity Theft Fraud exists in their various banks at all and if it does how often do it happen? The responses are presented in Table I.

Table 1. Determining the existence of Identity Fraud and rate of occurrence

S/N	Are their Identity theft /Issues in your bank?	Responses				How often do we have these issues?	Responses			
		Bank A	Bank B	Bank C	Total		Bank A	Bank B	Bank C	Total
1	Y	8	9	7	24	Not Often	9	8	8	25
2	N	4	3	6	13	Often	4	1	1	6
3	No Response	1	0		1	Very often	0	0		0
						No Response	0	3	4	7
	Total	13	12	13	38	**Total**	13	12	13	38

Table 1 translates to sixty-three (63) percent of the respondents with the opinion that there exist identity theft issues in their Banks while thirty-four (34) percent feels there are none. Three (3) percent did not respond at all.

Figure 1.



Chat showing percentages of existence of Identity Fraud in Banks

Sixty-six (66) percent of respondents answered not often to how often they have identity theft issues while eighteen (18) percent did not respond, "very often" option has zero (0) percent and the "Often" option sixteen (16) percent.

Figure 2.

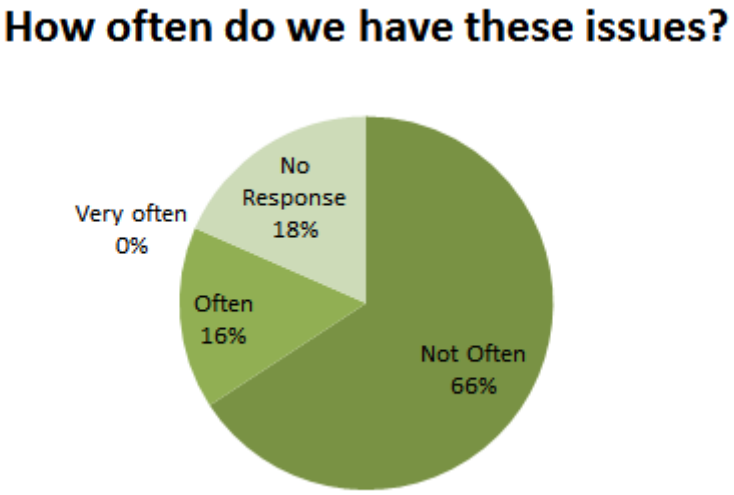


Chart showing have often we have Identity Fraud issues

From the total thirty-eight (38) responses from the two banks twenty-four (24) agreed that Identity Theft is indeed an issue in their banks and therefore answered in the affirmative, thirteen dissented while one (1) respondent did not respond to the question at all. Of the thirty-eight respondents twenty-five (25) are of the opinion that identity fraud does not happen often while six (6) feels it does happen often. Seven respondents did not respond to the question while none agreed with the "very often" option.

The next question is what are the major causes of identity fraud in your bank and will addition or review of controls against Identity Theft Fraud ensure more effectiveness? Respondents were required to pick Addition, Review or Both. The results are presented in table II.

Table 2. Determining the causes of Identity fraud in Banks

S/N	Major Causes of Identity Fraud in Your Bank	Responses				Will Addition or Review of Controls against Identity Fraud Theft Ensure More Effectiveness	Responses			
		Bank A	Bank B	Bank C	Total		Bank A	Bank B	Bank C	Total
1	Lack of controls	2	1	1	4	Addition	5	3	2	10
2	Lack of adequate controls	4	7	2	13	Review	6	1	4	11
3	Lack of proper implementation of controls by the bank	4	6	5	15	Both	2	8	4	12
4	Lack of abiding to controls/rules by the customer	6	5	7	17	No Response	0	0	3	3
5	Lack of awareness on the part of the customer	5	5	7	15					

In answering what are the major causes of identity fraud in your bank, twenty-seven (27) percent of respondents pick lack of abiding to controls/rules by the customer as the major cause of identity fraud in banks. This is followed by lack of proper implementation of controls by the bank 24%, lack of awareness on the part of the customer 23%, lack of adequate controls 20% and lack of controls 4%.

Figure 3.

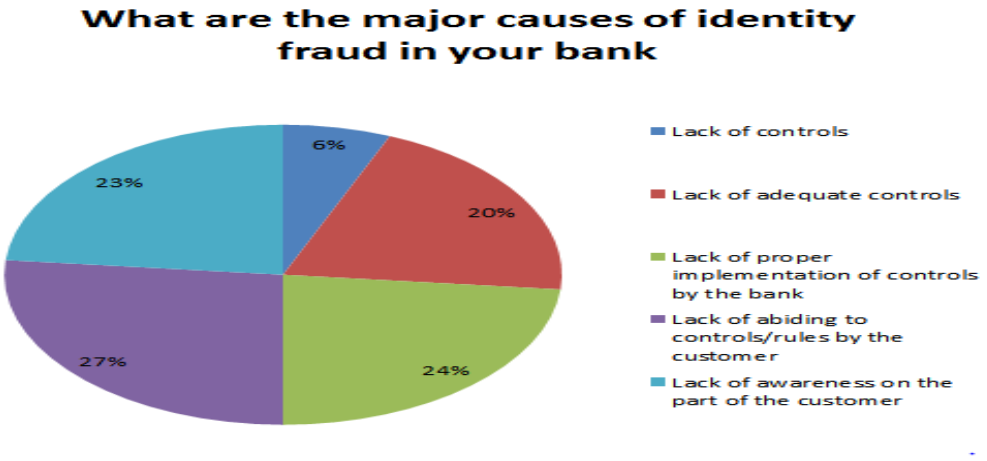


Chart showing various reasons for identity fraud in Banks

Five options were given to rate the major causes of identity fraud theft in Nigerian banks. Lack of abiding to controls/rules by the customer is the chief reason why identity thefts fester with seventeen (17) respondents. Next with fifteen respondents each is Lack of proper implementation of controls by the bank and Lack of awareness on the part of the customer. Lack of adequate controls is rated by thirteen (13) while Lack of controls trails with a total of four (4) responses.

The respondents in answering the question will addition or review of controls against identity fraud theft ensure more effectiveness? Choices both with 33% as depicted in figure.

Figure 4.

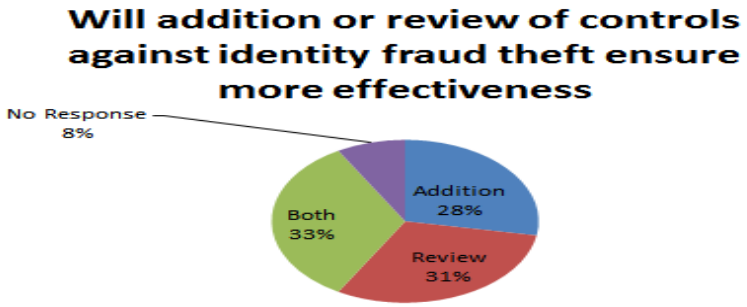


Chart showing whether more controls should be added by Banks

Captured next are the ranks of the respondents from the three (3) banks, their job role and opinion on how identity theft can be adequately reduced in the banks. This is labeled as table 3.

Table 3. Respondent's opinion on how to reduce Identity Fraud

S/N	Rank of respondent	Job role	How can Identity theft be adequately reduced in the bank?	Rank of respondent	Job Role	How can Identity theft be adequately reduced in the bank?	Rank of respondent	Job Role	How can Identity theft be adequately reduced in the bank?
	Bank A			**Bank B**			**Bank C**		
1	Entry Trainee	Data Analyst	Identity fraud can be reduced by proper training on security measures for both staff and customers	Entry Trainee	DB Admin	Put proper security in the environment and the system too			Sensitization of customers and staff in different languages on the ills of identity fraud
2	Assist. Mgr.	Network Support	Proper caution and rules should be stated	Assist. Mgr.	IS Audit	Review controls against identity fraud & implement additions. Continuous awareness should be pursued.			By educating both the customers and the bank staff
3	Executive Trainee	Compliance	Proper and adequate controls	Asst. banking Officer	System admin	Secure your social security number. Do not respond to unsolicited requests by mail or text message & phone calls. Instill & update firewalls & anti-virus. Store personal information in a safe place.			Strong credentials. Password review. User education &training
4	Banking Officer	Network admin	Constant review of controls and adequate sanctions for erring staff	Snr. Banking Officer	IT Auditor	Acquisition of identity management solution.			Proper enlightenment of risk associated and the need to abide with policies

5	Assist. Mgr.	Head, Data Center	Yes, putting in place necessary control policy	Asst. Mgr.	Information Security Officer	Effective monitoring of e-channels & continuous review of control awareness.			Staff enlightenment, proper staff compensation of bank controls
6	Banking Officer	Network Support	More awareness people should be more informed, and organization should have a good staff welfare.	Manager	Loans Operations	Review of controls regularly.			Customer awareness and acceptance
7	Banking Officer	Network Support	Educate the identity owners on the ways to safeguard their identity. Adequate controls in place and improvement on the security policies.			Constant education as re-education is required			Proper control measure and also full implementation
8	Executive Trainee	Regulatory compliance	Proper Control by the Management of the organization.			Review of controls and increase of alertness on the part of users.			Staff training. Rotation of job roles. Rotation of job roles. Customer awareness
9	Executive Assistant	Compliance	Ensure staff are well trained						By abiding to control measures put in place by the bank and by periodic reviewing all controls and policies
10	Executive Assistance	Regulatory Compliance	There must be adequate controls and proper implementation of controls.			If policies/punishments are adhered to and strictly followed			Improving the internal control and system control of the bank system
11	Assist. Mgr	Application Support	Adequate Control and customer awareness			A proper daily investigation by resident control of each branch			Observing due diligence

12	Banking Officer	Application Support	Information to all stakeholders. Putting adequate controls in place				Asst. Mgr.	Operations Mgr.	Enlightenment. More Controls. Regular upgrade of controls
13	OA	Regulatory Compliance	No response	Banking Officer	IT/Branch Support	By sensitizing public/individual on how to safeguard their identity both in official and private capacity			

The respondents with different ranks are drawn from several departments ranging from IT to Internal Control. They all offered different views in their responses on how to curtail the problem of identity theft.

Conclusion

From the results of this research study identity theft fraud does exist in Nigerian banks though it does not occur often. Lack of abiding to controls/rules by the customer is the major reason why identity theft fraud persists followed jointly and closely by lack of awareness on the part of the customer and lack of proper implementation of controls by the bank.

Generally, financial institutions such as banks are not open to research, but it is our duty as researchers to infiltrate them and dig out research worthy issues like this for the betterment of the overall society. Both banks as well as customers loss a lot of funds through the advent of fraudsters. With the rising profile of identity fraud as the fastest growing crime in the world, this work will foster further understanding of the intricacies within the banks and bring about the momentum for more solutions to be proffered by further exploration by other researchers.

Recommendations and Future Work

A major fact established in this paper is that Identity Theft does exist even though the banks may downplay such a fact. The following recommendations will assist the banks in dealing with some of their Identity fraud Issues:

- Becoming open to research works by allowing more researchers access to information as doing so will enable quality researches to be conducted that will assist the banks curtail their identity fraud challenges. This can be arrived at by signing strict MOU's that will ensure non-disclosure.
- Findings in this paper has highlighted lack of abiding to controls/rules by the customer, Lack of awareness on the part of the customer and lack of proper implementation of controls by the bank as the major causes of identity fraud in Nigerian banks. This means the banks blames the customer more than themselves, but they do agree that they do not administer enough control measures. The banks should ensure that they do more in the area of managing

their customers by developing a better customer education strategy & management as well as improve their staff efficiency while managing and implementing their control mechanisms.

- In cases where staffs or even customers are found engaging in fraud, the banks should ensure that proper punitive action is taken to serve as deterrent to others.
- To ensure that regular update and adequacy of controls exists in the banks they need to perform a thorough review and add more controls to the ones presently on ground.

For those who can circumvent the strict access problem in Nigerian Banks further research study from this paper includes:

- Investigating the depth of the bank's customer awareness program on IT fraud issues
- Taking into cognizance banks nag for secrecy concerning fraud cases in general and thereby not pressing charges, it will be apt to investigate thoroughness of how banks handle cases of staff and customers that are found to have committed frauds
- Investigating adequacy of IT staff training in banks compared to IT security and fraud incidents

References

Benbasat, I., Goldstein, D.,&Mead, M. (1987). The Case Research Strategy and Studies of Information Systems. MIS Quarterly, Vol 369 September 1987.

Bjorck., F. (2004). Institutional Theory: A New Perspective for Research into IS/IT Security in Organizations.

Brunsson, N. (1998). A world of standards: Standardization as a social form. Stockholm, Stockholms Centrum for Forskningom OffentligSektor Stockholms Universitet (Stockholm Center for Organizational Research Stockholm University).

Chinonye, J., Onyeagba, G. (2017). Internet Banking: Identity Theft and Solutions – The Nigerian Perspective. Journal of Internet Banking and Commerce. An open access Internet journal (http://www.icommercecentral.com) Journal of Internet Banking and Commerce, August 2017, vol. 22, no. 2.

D'Arcy, J., Gupta A., Tarafda, M., Turel, O. (2014). Reflecting on the 'dark side' of Information Technology use. Communications of the Association for Information System. Vol. 35.

Gregor, S. (2006). The Nature of Theory in Information Systems. MIS Quarterly Vol. 30 No. 3, pp. 611-642/September 2006.

Hedayati A. (2014). An analysis of identity theft: Motives, Related frauds, Techniques and Prevention. Journal of law and conflict resolution. http://www.academicjournals.org/article/article1379859409_Hedayati.pdf.

Kling, R. (1996) Computerization and Controversy: Value Conflicts and Social Choices (2nd edn), San Francisco, Morgan Kaufman.

Joel, C., Jason, G., Joseph, S., and Kageni, N. (2014). Identity Fraud: A Literature Review and Future Research Directions. Africa Development and Resources Research Institute Journal, Vol. 5, No. 5(2), Pp. 36-53.]

Monica NA (2013). Challenges of using IT to Combat Economic Crime. African J of Comp and ICTs 6: 31-36.

Scott, W. R. (2001). Institutions and organizations. Thousand Oaks, Calif., Sage Publications. Tarafdar, M., Gupta, A. &Turel, O. (2015). Special issue on 'dark side of information

technology use': an introduction and a framework for research. Information Systems Journal, 25, 161–170.

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. European Journal of Information Systems, 4(2), 74–81. https://doi.org/10.1057/ejis.1995.9

Walsham, G. (1993). Interpreting Information Systems in Organization. John Wiley & Sons Inc.