International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-3, Issue-3, May-2015

Fraud Management System in Detecting Fraud in Cellular Telephone Networks

Dr Isa Ali Ibrahim, I. B. Mohammed, Bashir Saidu

Abstract **-With fraud perpetrators becoming more sophisticated both in their techniques and the tools they use, fraud is an increasing problem. Telecommunications service providers are currently second only to banks in losing money through fraud. Investments in an integrated fraud management system pay off quickly even for operators of small networks. However, telecommunication fraud has been a major challenge to the growth of the industry. Different solutions and services have been employed to curb this menace in the mobile industry, but the more advanced the service or solution, the more susceptible it is to fraud. This study therefore presents a survey on the Critical Analysis of Significance of Fraud Management System in Detecting Fraud in Cellular Telephone Network in NIGERIA. A major services provided by Nigeria's mobile telecommunication company over a specified period of time and proffer suitable solutions to reduce fraud in this industry in order to restore the telecommunication subscriber's confidence in their mobile operators. A descriptive survey design was used. using convenient sampling technique (i.e. non-probability). The respondents were staff and management of GLOBACOM. Measurements of the study were done and subjected to rigorous data processing and analysis using simple percentage through relevant statistics computer software package called statistical package for social science (IBM-SPSS version 20.0), average mean and standard deviation was also used to determine the final justification regarding the research study under review. The findings of the research work revealed Fraud Management System (FMS) plays significance roles in detecting fraud in GSM industry. The study recommends that a longitudinal study to be carried out, so as to study the factual nature and quality of fraud management system in detecting fraud cellular telephone network in Nigeria's GSM industry.**

Index Terms**— Fraud management, cellular, GSM, telecommunication, unauthorized service**

I. INTRODUCTION

Fraud is a serious problem around the globe. The problem with telecommunication fraud is the huge loss of revenue and it can affect the credibility and performance of telecommunication companies (Akhter & Ahamad, 2012). The most difficult problem that faces the industry is the fact that fraud is dynamic. This means that whenever fraudsters feel that they will be detected they find other ways to circumvent security measures. Telecommunication fraud also involves the theft of services and deliberate abuse of voice and data networks. In such cases the perpetrators intention is to completely avoid or at least reduce the charges for using the services (Akhter & Ahamad, 2012). Over the years, fraud has increased to the extent that losses to telephone companies are measured in terms of billions of American dollars. Fraud negatively impacts on the telephone company in 4 ways; financially, marketing, customer relations and shareholder perceptions (Akhter & Ahamad, 2012).

Fraud permeates the whole sector of Nigeria's economy; the mobile telecommunication industry is no exception. Nigeria's mobile industry is one of the fastest growing sectors of her economy with increasing numbers of mobile telecommunication operators (Ogundile, 2013). However, telecommunication fraud has been a major hindrance to the rapid growth of this industry as it has caused both the telecommunication operators and its subscriber's loss of revenue. Different solutions and services have been employed to curb this menace in the mobile industry, but the more advanced the service or solution, the more susceptible it is to fraud (Ogundile, 2013). Therefore, this study focused on managing and detecting fraud in Globacom GSM Network service provider in Nigeria's mobile telecommunication industries over a specified period and proffer suitable solutions to reduce fraud in this industry in order to restore the telecommunication subscribers' confidence in their mobile operator.

Fraud is as old as humanity itself, and can take unlimited variety of forms. It occurs in so many areas, for example, telecommunication fraud, credit card fraud, internet transaction fraud, e-cash fraud, insurance fraud and healthcare fraud, money laundering, intrusion into computers or computer networks (Bolton & Hand, 2002). The task of detecting fraud is similar in all these areas.

Fraud is different from revenue leakage. Revenue leakage is characterized by the loss of revenues resulting from operational or technical loopholes where the resulting losses are sometimes recoverable and generally detected through audits or similar procedures. Fraud is characterized with theft by deception, typically characterized by evidence of intent where the resulting

Manuscript received May 25, 2015.

Dr Isa Ali Ibrahim, Assistant Professor, Faculty of Computer Science and Information Systems Islamic University of Madinah, 42351, Kingdom of Saudi Arabia

I. B. Mohammed, Lecturer, Department of Information Technology, Abubakar Tafawa - Balewa University, Bauchi.

Bashir Saidu, Lecturer, Department of Information Technology, Abubakar Tafawa - Balewa University, Bauchi.

losses are often not recoverable and may be detected by analysis of calling patterns (Bolton & Hand, 2002).

For any organization, having a secure network is one of the primary aims to reach their business goal. A network is said to be reliable when it can withstand attacks, which may damage part or a whole system. An ideal secure network should resist intrusion to the barest minimum (Grand, 2012). However, in practice, no network is hundred percent secure from intrusion attempts by intruders, either internally or externally. Intrusion attempt can still succeed, in spite of security measures in place. It is therefore imperative to detect intrusion and limit its effects on networks, as much as possible (Grand, 2012).

Furthermore, a survey has been conducted and determined that $72–$80 billion in losses are due to telecom fraud worldwide (CFCA, 2009). While many large operators have developed sturdy, Fraud Management Systems (FMS) to combat fraud, others have not. The Forum for International Irregular Network Access (FIINA) concluded that perhaps only about 10% of operators worldwide have set in place sensible and effective fraud strategies (Shalton, 2003).

The motivation behind crime is attributed to migration and demographics, penetration of new technology, staff dissatisfaction, the 'challenge factor', operational weaknesses, poor business models, criminal greed, money laundering and political and ideological factors (Brown, 2005).

A Statement of the Problem

Dealing with the fraud is a very complex task mainly due to its transversal nature to the operators' structure (Samarati, 2010). With fraud perpetrators becoming more sophisticated both in their techniques and their tools, fraud is an increasing problem.

Telecommunications service providers are currently second only to banks in losing money through fraud (Samarati, 2010). Experience shows that if no effective anti-fraud control exists, sooner or later an operator will be hit by a major fraud problem (Kapsch, 2014). So as the number of subscribers, distribution channels, and enhanced services grow, and more complex tariff structures are put in place, an effective fraud management system is now essential to minimize losses. Investments in an integrated fraud management system pay off quickly even for operators of small networks (Kapsch, 2014).

Deceptions in telecommunications include subscription frauds where the cheater accesses the services without being subscribed. User can also suffer line or identity theft being charged for services used by others (Akhter & Ahamad, 2012). Telecommunication operators can oversee users that exceed their download quote and rate performing illegal service redistribution, sometimes for an economic profit. Finally cloning or unauthorized access to services may lead to compromising privacy (Akhter & Ahamad, 2012).

B. Objectives of the Study

The general objective of the study is to ascertain the significance of Fraud Management System (FMS) in GSM industry by ensuring the following specific objectives:

i. To examine the roles of Fraud Management System (FMS) in protecting the GSM brand image and revenue streams from loss through internal and external fraud;

ii. To examine the benefits of Fraud Management System (FMS) that enables a continuous cycle of detection and prevention of fraud management; and

iii. To identify the difficulties in detecting fraud in GSM Network.

C. *Research Question*

What are the roles of Fraud Management System in protecting the GSM brand image and revenue streams from loss through internal and external fraud?

D. Significance of the Study

Fraud remains serious global issue for mobile network services despite improvement in security technology. While recent development have enhanced some capabilities and filled known security holes, fraudsters have been nimble enough to seek alternative techniques that minimize detection with current technologies, so there is great need of high awareness in facing fraud phenomena. The importance of this study is focusing on fraud threads directing to telecommunication operators operating in Nigeria and many developing nations, due to the fact that there are no enough studies that focusing on fraud generally and fraud detection in cellular communications especially throughout the operators working in the Nigeria. This study may assists in trying to protect the revenue of GSM operator and minimize the operators' exposure to fraud.

II. LITERATURE REVIEW

Many definitions in the relevant literature exist, where the intention of the subscriber plays a central role. Johnson defines fraud as any transmission of voice data across a telecommunications network, where the intent of the sender is to avoid or reduce legitimate call charges (Hollmen, 2000). In similar veins, fraud is defined as obtaining unbuildable services and nude-served fees (Hollmen, 2000). Hoath considers fraud as attractive from fraudster's point of view, since detection risk is low, no special equipment is needed, and product in question is easily converted to cash **(**Hollmen, 2000). Although the term fraud has particular meaning in legislation, this established term is used broadly to mean, misuse, dishonest intention or improper conduct without implying any legal consequences. Fraud is a problem for all businesses (KPMG's, 2002).

The telecommunication industry has expanded dramatically in the last few years with the development of affordable mobile phone technology (Pieprzyk et al., 2007). With the increasing number of mobile phone subscribers, global mobile phone fraud is also set to rise. It is a worldwide problem with substantial annual revenue losses of many companies. Telecommunication fraud which is the focus is appealing particularly to fraudsters as calling from the mobile terminal is not bound to a physical location and it is easy to get a subscription. This provides a means for illegal high profit business for fraudsters requiring minimal investment and relatively low risk of getting caught (Akhter & Ahamad, 2012). Telecommunication fraud is defined as

the unauthorized use, tampering or manipulation of a mobile phone or service (Akhter & Ahamad, 2012).

At the beginning of the twenty first century, the convergence of computing and communication technologies has altered considerably the way in which industrialized communities function. It has created unfold benefits for education, delivery of health services, recreation and commerce and changed considerably the nature of modern workplaces and patterns of employment (Akhter & Ahamad, 2012).

In addition, telecommunication fraud can be simply described as any activity by which telecommunications service is obtained without intention of paying. This kind of fraud has certain characteristics that make it particularly attractive to fraudsters (Akhter & Ahamad, 2012). The main one is that the danger of localization is small. This is because all actions are performed from a distance which in conjunction with the mess topology and the size of network makes the process of localization time consuming and expensive (Akhter & Ahamad, 2012).

Additionally, no particularly sophisticated equipment is needed if one is needed at all. The simple knowledge of an access code, which can be acquired even with methods of social engineering, makes the implementation of fraud feasible. Finally the product of telecommunication fraud, a phone call is directly convertible to money (Akhter & Ahamad, 2012).

Fraud as part of the revenue assurance capability, linked with security or stand alone there is no right or wrong approach. Fraud Management is about minimizing exposure, detecting illegal activities and implementing effective controls so that fraud is harder to perpetrate in the future (Graycar & Smith, 2002). Fraud Management is about making the network and business operations safer, ensuring top management that the fraud phenomenon is understood and being kept under control.

Furthermore, the objectives of fraud management are easier to understand and to "sell" to the business than other aspects of risk management. Fraud Management will detect and prevent fraudulent activities in all areas under its remit, operate in line with the powers mandated by executive management, act quickly on discovered instances of fraud to stem losses, produces effective controls, monitoring capabilities and preventative actions in order to diminish the exploitation risk measure, report on and escalate issues and track the resolution when appropriate. Fraud management is not a collection or credit control department or an internal audit department (Graycar & smith, 2002).

Consequently, fraud losses continue to impact virtually every business enterprise, despite significant advances in fraud detection technology, fraud losses continue to pose a significant problem to many finance, insurance, health care, internet merchants, brokerage and securities, and many others, about the telecom companies We can only estimate the cost because operators are reluctant to admit to fraud or are not actively looking for fraudulent accounts in the bad debt (Goliath, 2004), also the business driver is for subscriber growth and market share, therefore, the fact that huge number of the new customers could actually be fraudsters is not taken into consideration.

Similarly, responsibility for chasing unpaid bills is spread across a variety of departments which could include billing, IT, fraud, credit management, customer service, collections and the finance departments, this often results in an ineffective ability to collect debts and a1so does not help identify fraud as skills are not present in all business areas to identify fraudsters as opposed to bad debtors (Federal register, 2008).

In addition, increased innovation in telecommunication fuels more fraud also increased competition provides more avenues of attack, increased mobility also means fraudsters are harder to track down and internationally organized. In survey conducted by communication control fraud association (CFCA), including 123 operators and more than 30 countries worldwide, the survey estimated the global fraud loss as 72-80 billion (USD) annually (34% increase from 2005 to 2010) (Kumar, 2010).

Networks do not or cannot distinguish between fraud and bad debt (Business issue, 2009). Prepaid , internal and interconnect/bypass fraud is rarely included in the reported figures Areas unrelated to airtime loss are not included such as theft, subsidy and commission payments and the cost of customer acquisition etc (Nokia Siemens network, 2008).

Mobile telecommunication fraud refers to illegal access to the mobile operator's network, using their services for unlawful interest to the detriment of the network operators and/or its subscribers. Fraud is the principal profit leakage area in the mobile telecommunication industry (Wieland, 2004). In fact, it was estimated globally that mobile telecommunication fraud cause losses of tens of billions of dollars yearly (FML, 2003).

Unfortunately, fraud exists in every operator in every country throughout the world there is no exceptions, committing fraud does not need highly complex equipment or skills, fraudsters are normally lazy people. Fraudulent application for service is the first step in achieving illegal access to network services, Fraudsters prey on operator's weaknesses in their controls and procedures. In a recent survey 85% of the communications operators surveyed stated that global fraud losses have increased or stayed the same (CFCA, 2006). All operators will suffer from some internal fraud at some point irrespective of whether they believe their employees are all honest and trustworthy (Kroll, 2009).Top 5 Countries where fraud was concentrated were Pakistan, Philippines, Cuba, India and Bangladesh, Cuba being the newest member to the top 5 lists (CFCA, 2006).

A. Reasons behind perpetrating the Fraud

Fraud has and can be committed by any type of person in society Albrecht et al. (Anonmyous, 2003), whatever the social status, nationality, or position/role within the business, If they have the driver (initiative, desire. Commitment, purpose etc) they will find the way and means to commit fraud, no one is exempted. However the followings are the major reasons why peoples commit fraud:

i. To make money (Revenue Fraud), for example, by selling fraudulently obtained telephone services at cheap rates;
ii. By avoiding or reducing payment of services used, (Non-Revenue Fraud); and

iii. Demonstrating ability to outmanoeuvre the service provider's system security, (Johnson, 2002).

B. Telecoms Fraud Types

The types and severity of fraud attacks will primarily revolve around the market environment the CSP is operating within and will relate to the range of products and services being offered or planned for. CSPs have business plans in place to determine the innovative products they will provide to the respective customer segments (corporate, business and residential). The criminal fraternity is also actively determining their own business strategy" for defrauding what is provided (Praesidium, 2011). The followings are some common types of fraud:

i. Subscription Fraud Usage
ii. Airtime Fraud
iii. Unauthorized Service Fraud
iv. Sales and Dealer Fraud
v. Internal Frauds

C. Benefits of a Fraud Management System

Essentially, the FMS processes data from the CSP and its partners and applies a number of different rules, profiles and data analytics to verify if the customer, employee, dealer or third party is using the CSP's network and services to commit fraud. Hence, the followings are Benefits of a Fraud Management System (Praesidium, 2011).

i. **Automation:** The extraction and processing of the relevant events is performed with little or no human intervention. The FMS has the ability to interface to many different data sources to ensure visibility and coverage of usage on a wide range of products and services.
ii. **Volume and Quality of Data:** The volume of data a dedicated FMS can process is typically far in excess of any that a homegrown solution developed within a CSP can handle. The quality of data used and monitored within FMS is also high since it is usually retrieved directly from the sources or a mediation platform. This in turn produces a high level of clarity on what the origin of the data was, therefore assuring that frauds identified are based on accurate and reliable data.
iii. **Flexibility:** FMS have to be flexible in their ability to take any type of data feed and to create flexible rules on any type of event to address the changing dynamics of fraud today and to address future fraud threats in next generation technologies and products & services. This flexibility is a major asset for the Fraud Analysts as it provides the capability to test and verify various thresholds and alarm settings to maximize their capabilities of fraud detection.
iv. **Dashboard:** A dashboard view of the level and nature of fraud being detected within the FMS, visible in one screen is a key tool for a Fraud Manager. This allows the Fraud Manager to view key performance indicators (KPIs), assess whether fraud detection targets are being met, and review the performance of the Fraud Analysts to ensure cases are being managed and resolved in a timely manner. Ultimately this enables the Fraud Manager to determine whether the FMS performance and resources are both operating in line with the fraud strategy and providing the required ROI.
v. **Case Management:** An integrated Case Management tool ensures all fraud incidents identified are recorded and tracked in a centralized location. This historical information can then be used to identify organized fraud syndicates and repeat fraudsters, where links are identified between new and old cases. In addition, it ensures that all information relating to a case can be stored for ease of retrieval at a later stage. This is essential when managing fraud where investigation or evidential case papers may be required for legal purposes or for review during internal audits. It also enables the Fraud Manager to track and monitor performance of the Fraud Analyst cases to ensure defined standards and processes are being met and adhered to.

III. RESEARCH METHODOLOGY

This section deals with the practical procedure that was used in carrying out the study. It gives details of the research design to be adopted, population of study, nature of sample, sampling procedures, and sample size, response rate, sources of data, method of data collection and finally, method of data analysis technique that was applied. It gives the framework within which data was collected and analysed.

A. Research Design

The objective of this study is to focus on how GSM Operators managing and detecting the fraud, (A case study of GLOBACOM branch). A descriptive survey design was used to provide details of interest at a single point in time. Research design is a plan which specified how data relating to a given problem should be collected and analysed.
Consequently, quantitative data was used to describe the statistics of the scores using indices that described the current situation and investigated the associations between the study variables using information gained from the questionnaires.

B. Population of the Study

The population defines the limit within which the research findings were acceptable, for the purpose of this research work; the population of the study was the management and staff of GLOBACOM for comprehensive analysis which is 43. Out of 43 questionnaires that were distributed, 40 questionnaires were correctly filed and collected.

C. Sample Size and Response Rate

The sample size of the study was determined using convenient sampling technique, which the total of correctly filled and returned questionnaires were used and was 40**.** This assumption was that the sample was a representative of the population. The rate of about 90% of the total questionnaires was administered.

D. Sampling Technique and Sources of Data

The sampling of research work was carried out using convenient sampling technique (non-probability).
For the purpose of this research work, the research by reason of the nature of the project work under review basically constitutes the use of primary data, which was

obtained through the use of self –administered questionnaires to respondents following systematic and established academic procedures, as suggested by (Anderson, 1988 and Nunnally & Bernstein, 1994). On the other hand, secondary data was obtained through the already existing transparent information gathering which includes articles, journals, textbooks and reports.

E. Method of Data Collection

For the purpose of the research work, the questionnaires were validated. The questionnaire method was used to ensure the high rates of response, as well as allowing for clarification of possible ambiguities related to questions asked (Churchill, 1995). The questionnaire contained statements that reflect the research problems and sought answer to the research questions. The questions addressed the roles of Fraud Management System in GSM industry and the need of it in that industry. The respondents were management and staff of the GLOBACOMM.

A five (5) point likert scale was constructed to test the differences between the various factors ranging from Strongly Disagree (1 point), Disagree (2 points), Undecide (3 points), Agree (4 points), Strongly Agree (5 points) was adopted for the study.

F. Method of Data Analysis

Data from the field was compiled, sorted, numbered and coded to have the required quality, accuracy and completeness. Then entered into the computer using the IBM Statistical Package for Social Sciences (IBM SPSS version 20.0) During the analysis of the data, descriptive statistics were used to present the results of the sample characteristics, this includes the use of frequencies percentages of measure of central tendency (Mean and Standard Deviation) to analyse data that was collected.

The following mean formula was used to determine if the respondents were bias or not in their response.

Mean

$$\bar{x} = \frac{\sum fx}{N}$$

Therefore, $\sum fx$ = summation of frequency

N = number of frequency

$\bar{x}$ = ?

$$\bar{x} = x \quad \frac{5 + 4 + 3 + 2 + 1 = 3}{5}$$

This implied that any research question item with mean score of 3.0 and above will be accepted, while any research question item with mean score less than 2.99 will be rejected. However, the mean and standard deviation was used to determine the final justification regarding the research study under review.

IV. DATA PRESENTATION AND ANALYSIS

The comprises of data presentation of results in a text and tabulation form, analysis of data presented earlier and the results after the calculations were made through frequencies percentage and measure of central tendency and followed by the interpretation of the analyzed data in brief note. In addition, this is based on the implication of the decision of the respondents. The presentation shows the results as tested according to the objectives of the study.

Table 1 Examining the roles of Fraud Management System (FMS) in protecting the GSM brand image and revenue streams from loss through internal and external fraud.

Number of Respondents (N = 40)									
S/N	**Questionnaire Items**	**SA (5)**	**A (4)**	**U (3)**	**D (2)**	**SD (1)**	**Mean $\bar{x}$**	**Std. Dev**	**Remark**
1	Fraud Management System aids in developing policies, strategies and procedures to ensure that all identified frauds are managed within the GSM industry.	32	7	-	1	-	4.75	0.59	Strongly Agree
2	Fraud Management System plays an important role in reviewing and analyzing frauds.	28	10	1	-	1	4.60	0.78	Strongly Agree
3	Fraud Management System provides strong indication for identifying, assessing and managing fraud.	28	9	2	-	1	4.58	0.81	Strongly Agree
4	Fraud Management System aids in customization of fraud detection sensitive and for alarm filtering.	26	10	4	-	-	4.55	0.68	Strongly Agree
5	Fraud Management System enables the fraud manager to track and monitor performance of the fraud analyst cases to ensure defined standards and processes are being met and adhered to.	24	12	3	1	-	4.48	0.75	Agree
Average							4.60	0.72	

Source: **Field Survey, 2015.**

As shown on the Table 4.9, respondents were strongly agreed on items number 1, 2, 3, 4, and 5 agreed with their average mean of 4.60 and average standard deviation of 0.72 respectively. From the above analysis, it can be deduced that fraud management system safeguards, managed and also improve integrity of GSM industry in their operations.

A. Summary of the Findings

Under this section, based on the analysis of the available data, summary of the findings was presented in accordance with the study objectives. It was however, discovered that:
Table 1 depicted that fraud management system safeguards, managed and also improve integrity of GSM industry in their operations. This finding is based on the respondents' responses.

V. SUMMARY, CONCLUSION AND RECOMMENDATIONS

This chapter presents the summary of the findings, conclusions and recommendations arising from the research findings in Chapter 4 and suggests areas for further study. The study has generated several findings which are in line with objectives of the study.
Fraud has indisputably become a significant cause of substantial annual revenue losses in Nigeria's mobile telecommunication industry. If proper fraud detection technology is not put in place by each network operator and NCC to curb this menace, it will lower the subscribers' confidence in the security of transactions available via the service operator.

A. Recommendation

The battle against fraudsters can never be won or can never be finished completely due to the fast moving telecoms environment and the drive to launch more complex products and services quickly to attract market share and maintain a competitive advantage. This will always lead to procedural weaknesses and technical risks being introduced which fraudsters will seize upon at the earliest opportunity to keep their fraudulent 'business' activities operational and profits high.
However, CSPs can deploy various defence mechanisms such as Fraud Management System (FMS) to mitigate against losses and ensure fast detection by ensuring processes are continually reviewed, staff are educated in new fraud trends, new products and services are assessed for fraud and security weaknesses and state of the art technology is used to quickly raise alerts for suspect activity.

REFERENCES

[1] ACFE. (2006). The report to the nation on the occupational fraud and abuse, technical report. Association for financial prepositional, payment fraud survey, report of survey result, underwritten by electronic payments network. Retrieved on 26 July 2014, from http://www.afponline.org/pub/pdf/2007PaymentsFraudSurvey.pdf.

[2] Agrawal, A P. (2010).Telecom fraud management. Retrieved on 26 July 2014, from http://www.cerebralbusiness.com/telecom/presentations/Arpita%20Pal%20Agrawal.pdf,

[3] Akhter, M., I., Ahamad, M., G. (2012). Detecting Telecommunication Fraud using Neural
Networks through Data Mining. International Journal of Scientific & Engineering Research, Volume 3, Issue 3.

[4] Allen, L. (2010). Fraud and social engineering in community bank, information security trends and strategies. Retrieved on 26 July 2014, from http://www.larsonallen.com/Advisory_Services/Fraud_and_Social_Engineering_in_Community_Banks.aspx

[5] Anonymous. (2003). Who commit fraud and why. Retrieved on 26 July 2014, from http://www.swlearning.com/pdfs/chapter/053872689X_2.PDF.

[6] Apri.(2004).Experience of fighting telecommunication fraud. Retrieved on 26 July 2014, http://www.nadaaapri.org/pdf/sounds tppgood.pdf,

[7] A&T. (2009). Business subscription and equipment fraud prevention. Retrieved on 26 July 2014, from http://www.atlantacellular.com/posdotcom.

[8] Baker, T. (2008). Anti – fraud management survey results, magnify your anti fraud managemen. Retrieved on 12 July 2014, from http://www.bakertilly.com/cms/public.

[9] Banjoko, A. (2009). Using the circle of trust to enhance fraud management in developing markets, GRAPA. Retrieved on 26 July 2014, from www.telecom-fraud.org,

[10]Bavosa, A. (2004). GPRS Security threats and solution recommendations. Juniper network, white paper. Retrieved on 26 July 2014, from http://stools1. juniper.net/solutions/literature/ white_papers/200074.

[11] B/OSS. (2004).Telecom fraud on raise. Retrieved on 26 July 2014, from http://www.billingworld.com/articles/2004/07/telecom-fraud-on-the-rise .aspx.

[12] B/OSS. (2007).Top telecom fraud and how to stop them. Retrieved on 26 July 2014, from :http://www.billingworld.com/articles2007/01/top-telco-frauds-and-how -tostop- them.aspx ,

[13] Business issue. (2009). Credit risk and bad debit, understanding receivables management problems and solutions for telecommunication , media and entertainment sector. Retrieved on 26 July 2014, from http://www.scribd.com/doc/28155799/Credit-Risk-and-Bad-Debt-in-Te lecommunications,

[14] Brown, S. (2005). Telecommunication fraud management. Retrieved on 26 July 2014, from http://waveroad.ca/ressources/Whitepaper_SB_Janvier2005.pdf.

[15]Brown, D. (2005). Southern African network an application conference. Retrieved on 12 June 2014, from http://mo.co.za/open/ngnfms.pdf.

[16] CFCA. (2009). Communication fraud control association results of worldwide telecom fraud survey. Retrieved on 26 July 2014, from http://www.cfca.org/pdf/survey/2009%20Global%20Fraud%20Loss%2 0Survey Press%20Release.pdf

[17]CFCA. (2006). Communication fraud control association results of worldwide telecom fraud survey. Retrieved on 14 July 2014, from http://www.cfca.org/pdf/press/3-28-06PR.pdf,

[18] Churchill H.(1995). General and Industrial Management, Pitman and Sons Press, London.

[19] Federal register. (2008). Department of labor, Employment standard and administration wages and hour division. vol.73.no.28. Retrieved on 26 July 2014, from http://www.dol.gov/whd/fmla/FedRegNPRM.pdf.

[20] Field, A.P. (2005). Discovering Statistics Using SPSS, 2nd Edition, London, Sage.

[21] FSA. (2006). Financial service authority, firms high –level management of fraud risk. Retrieved on 26 July 2014,from http://www.fsa.gov.uk/pubs/other/fraud_risk.pdf

[22] Goliath. (2004).Why customer churn. Retrieved on 26 July 2014, from http://goliath.ecnext.com/coms2/gi_0198-373341/4-Why-customersch urn.Html.

[23] Gonzalez-Castano, F.J., Vales-Alonso J., Pousada- Carballo, J.M. de Vicente, F.I.

[24] Fernandez-Iglesias, M.J., Taylor F. (2009), "Real-Time Interception Systems for the GSM Protocol," IEEE Transactions on Vehicular Technology, Vol.51, No.5, (pp. 904-914).

[25] Grandhi, S. (2010). Application of data mining to credit card fraud. Retrieved on 26 July 2014, from http://www.sas.com/offices.

[26] Grant, T. (2010).Trust and occupational fraud, how to trust is just as important as who to trust. white paper. Retrieved on 26 July 2014, from http://www.grantthornton.ca/resources/insights/white_papers/Trust_an d_occupational_fraud_2010_electronic.pdf,

[27] Graycar, A., Smith, R. (2002). Identifying and Responding to Electronic fraud Risk. Australian institute of Criminology, proceeding of the 30th Australian Registers conference Canbera Retrieved on 26 July 2014, from

[28] GSM Association. (2008). Mobile Roaming Service in Latin America, Market &technical approach .IIRSA Workshop .Bogota, Colombia. Retrieved on 21 July 2014, from http://www.iirsa.org/BancoMedios/Documentos%20PDF/tir_bo gota08_medidas_tecnicas.pdf.

[29] Hoath, P. (2008). Fraud overview, TAF regional seminar on cost and tariffs. Retrieved on 26 July 2014, from http://www.itu.int/ITU-D/finance/work-cost-tariffs/events/tariff-s eminars/djibouti-08/Peter%20Hoath-4-EN.PDF.

[30] Heerde, J H V. (2005). Detecting fraud in cellular telephone network. M S Theses. University of Stellenbosch ,south Africa. Retrieved on 10 July 2014, from http://dip.sun.ac.za/~vuuren/Theses/vanHeerden.pdf.

[31] Hollmen, J. (2000). User profiling and classification for fraud detection in mobile communication networks. M S. Thesis. Helsinki university of technology. Retrieved on 26 July 2014, from http://citeseerx.ist.psu.edu/viewdoc.

[32] Johnson, M. (2002). Future fraud, telecom fraud in the next generation service. Retrieved on 26 July 2014, from http://www.oct.ict.org/index.php?dir=4

[33] Johnson, M. (2002). Revenues assurance, fraud &security in 3G service. Journal of economics and crime. vol 1 issue 2, Retrieved on 26 July 2014, from http://www.utica.edu/academic/institutes/ecii/publications/articl es/BA2A7651-0488-

[34] Katzs, N. (2010). Protect again procurement fraud, Inside supply management.vol .21,No.3, page 16 Retrieved on 14 June 2014, from http://www.supplychainfraud.com

[35] KPMG. (2006). India fraud survey report. Retrieved on 12 August 2014, from http://www.in.kpmg.com/TL_Files/Pictures/Fraud_Survey_New .pdf ,

[36] KPMG. (2009). Revenue assurance in telecommunication progressing and preserving, global revenue assurance survey results. Retrieved on 26 July 2014, from http://www.kpmg.com/Global/en

[37] Krenker, A. Volk, M. Sedlar, U. Bester, J. & Kos, A. (2009). Bidirectional Artificial Neural Network For Mobile Phone Fraud Detection. Retrieved on 26 July 2014, from http://www.ltfe.org/wpcontent/

[38] Kroll. (2010). The Downturn and Fraud, your sector may even be better off. Retrieved on 14 Agust 2014, from http://www.kroll.com/about/library/fraud

[39] Kumar, M. Grifinkel, T. Bonen, D. Winorad T. (2010). Reducing shoulder surfing by using gaze-password entry. Stanford University. Retrieved on 26 July 2014, from http://www.stanford.edu.

[40] kumar, R. (2010). Fraud management system-selection and retuning ,unior. Retrieved on 26 July 2014, from http://www.cerebralbusiness.com/telecom.

[41] National fraud authority. (2010). Annual fraud indicator. Retrieved on 26 July 2014, from http://www.attorneygeneral.gov.uk/nfa/GuidetoInformation/Doc uments.

[42] Nelsson, O. (2009).Subscription fraud in telecommunication using detection tree learning. M .S. Thesis .Maker ere University. Retrieved on 26 July 2014, from http://dspace.mak.ac.ug/bitstream.

[43] Ogundile, O. (|2013). Fraud Analysis in Nigeria's Mobile Telecommunication Industry. International Journal of Scientific and Research Publications, Volume 3, Issue 2.

[44] Pieprzyk, J. Ghodosi, H. & Dawson, E. (2007). Information security and privacy: 12th Australasian conference, ACISP 2007, Townsville, Australia, July 2-4, 2007: proceedings, Springer, Germany, pp 446-447.

[45] Robert, R. Dabija, D. (2009). Telecom fraud management training course. Retrieved on 26 July 2014, from Praesidium,Qtel.

[46] Samarati, P. (2010). Information Security Theory and Practices: Security and Privacy of Pervasive Systems and Smart Devices: 4th IFIP WG 11.2 International Workshop, WISTP 2010, Passau, Germany, April 12-14, 2010, Proceedings, Springer, USA, pp 201.

[47] Shelton, R. (2003). The Global Battle against Telecommunication Fraud. Retrieved on 17 June 2014, from www.satnac.org.za/proceedings/2003/plenary/Shelton.pdf ,.

[48] Srinivas, S. (2001) "The GSM standard-An overview of it security" Sans Institute information Science Reading room, (Pp3), Retrieved June 21st, 2014. http;//www.isaac.csBerkeley-Edd- Edu/lsaac/gsm.html.

[49] Wilhelm, K., W. (2004). The fraud management life cycle theory, Holistic Approach to fraud management. Journal of economic crime management .Vol. 2,Issue2. Retrieved on 27 August 2014, from http://www.utica.edu/academic

[50] Yates, C. (2003). Mobile phone issues-what risks associated with their use by our youth. Retrieved on 08 July 2014, from http://www.netsafe.org.nz/DocLibrary/netsafe papers colinyates_mobile.pdf.

View publication stats