International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 25 No. 3 Feb. 2019, pp. 940-947

http://www.ijias.issr-journals.org/

GLOBAL TELECOMMUNICATIONS FRAUD TREND ANALYSIS

Godfred Yaw Koi-Akrofi[1], Joyce Koi-Akrofi[2], Daniel Adjei Odai[3], and Eric Okyere Twum[4]

[1]Senior Lecturer, Department of Information Technology, University of Professional Studies, Accra (UPSA), Accra, Ghana

[2]Programmes Manager, Vodafone Ghana, Accra, Ghana

[3]Telecom Engineer, Vodafone Ghana, Accra, Ghana

[4]Systems Administrator, AccuID Biometrics Ltd. (MoFEP Project), Ghana

ABSTRACT: The yearly global percentage fraud loss was on the downward trend, with only 2013 being an abnormal case. Again, telecom revenues went up gradually from 2008 to 2017. PBX hacking and Subscription fraud appeared for all the years (2013 to 2017) in the top 5 fraud methods, and for fraud types, subscriber/identity (ID) theft was prevalent in 2008 and 2011 but did not show up in the top 5 for 2013, 2015, and 2017. Rather, lately, that is from 2011 to 2017, interconnect bypass fraud and International Revenue Share Fraud (IRSF) have become prevalent. Five fraud types and methods stand out: Subscription Fraud, PBX Fraud, Subscriber/Identity (ID) theft, Interconnect Bypass Fraud (IRSF), and International Revenue Share Fraud.

KEYWORDS: Fraud, loss, revenue, telecommunications, trend.

1 BACKGROUND

Subsequent to the enormous growth in the end of the past century, the telecommunications operators face a new challenge: fraud. Fraud is a continuously changing, multi-facetted creature [1]. Telecommunications fraud are many (PBX/Voice mail systems, subscription/identity (ID) theft, International revenue share fraud(IRSF), credit card fraud, and so on) and new ones evolving every now and then. Telecommunications fraud is a big issue to all telcos around the world, and is an important factor in their annual revenue losses [2]. The issue of telecoms fraud and its detection have been studied over the years and all over the world, by the telcos, having spent so much money and time in it, than even the research community [3].

1.1 DEFINITION OF TELECOMMUNICATIONS FRAUD

In simple terms, any activity by which service is obtained without intention of paying is telecommunications fraud [1]. In other words, any attempt to benefit from the services of a telco without having to pay anything or paying less than the actual cost is telecommunications fraud. Researchers in literature have defined telecommunications fraud in many ways, and some are reviewed in this work.

According to Neustar, telecommunication fraud is defined as the stealing of telecommunication services or the use of telecommunication service to commit other forms of fraud [4, 5]. This definition introduces another aspect which most researchers overlook; that is the use of the telecommunications service to perpetrate fraud. In this instance, it may not be a loss to the telco, but a loss to a third party.

Johnson was a little bit technical in his definition when he said that telecommunications fraud is any transmission of voice or data across a telecommunications network where the intent of the sender is to avoid or reduce legitimate call charges [6].

Johnson's definition only tackles fraud from the originating point; it leaves out fraud at the receiving or terminating end, which is also widespread or prevalent these days.

Telecommunications fraud can also be seen as obtaining unbillable services and unmerited or unjustifiable fees [7]. The serious fraudster sees himself as a businessperson, undoubtedly making use of illicit or unlawful methods, but driven and directed by basically the same issues of cost, marketing, pricing, network design and operations as any legitimate network operator [6].

Telecommunications fraud is viewed as an appealing endeavor from the fraudsters' perspective, since detection is low, no exceptional hardware is required, and the product in question is effectively changed to money [8].

Another twist to the definition of telecommunications fraud is when there is abuse of voice or data networks [9]. This is more common with employees of Telecommunications companies; because they do not pay for the services in most cases, they abuse it to the disadvantage of their companies. In all these definitions, the subscriber is pivotal or plays an important role.

1.2 BRIEF HISTORICAL ACCOUNT OF TELECOMMUNICATIONS FRAUD

In the early stages of telecommunication's fraud, the method commonly employed was the use of technological means to acquire free access [10]. What was used to gain access was the cloning of mobile phones necessitated by creating copies of mobile terminals with identification numbers from genuine subscribers [7]. Capturing was achieved by eavesdropping or snooping, an easiest way of identifying numbers in the analog mobile terminal era, with appropriate receiver equipment in public places, where mobile phones were obviously used. In the United States, tumbling, a particular type of fraud was quite widespread [7]. The tumbling and cloning fraud have been severe threats to operators' revenues [7], and as a means to combat them, technological improvements were adopted.

Later on new forms of fraud emerged; significant among them was the subscription fraud. The subscription fraud was the trendiest and the fastest-growing type of fraud [11].

1.3 REVIEW OF LITERATURE

[1] Classify fraud into four groups: **Contractual Fraud-** with this fraud category, revenue is generated through the normal use of a service whilst having no intention of paying for use. Examples of such fraud are Subscription fraud and Premium Rate fraud; **Hacking fraud** – in this category, revenue is generated for the fraudster by breaking into insecure systems, and exploiting or selling on any available functionality. Examples of such fraud are PABX fraud and Network attack; **Technical fraud** - all frauds in this category involve attacks against weaknesses in the technology of the mobile system. Such frauds typically need some initial technical knowledge and ability, although once a weakness has been exposed this information is often quickly distributed in a form that non-technical people can use. Examples of such fraud are Cloning, Technical Internal fraud; **Procedural fraud** - all frauds in this category involve attacks against the procedures employed to minimize exposure to fraud, and often attack the weaknesses in the business procedures used to grant access to the system. Examples of such fraud are Roaming fraud, Voucher ID duplication, and Faulty vouchers.

Telecommunications fraud can be divided into several wide-ranging classes, these classes depict the mode in which the operator was defrauded, for instance, subscription exploiting false personality. Every mode can be exploited to cheat the system for income based purposes or non-income based purposes. A large portion of these cheats are executed either by the fraudster imitating another person or in fact deluding the network systems [12].

[13] also grouped telecom fraud into fraud types and fraud methods. The fraud types include arbitrage, call and SMS spamming, domestic revenue share fraud, international revenue share fraud, phishing, premium rate service fraud, roaming fraud, and so on, the fraud methods include cramming/slamming, PBX Hacking, SMS Phishing, Subscription Fraud, Wangiri Fraud, and so on. These fraud types and methods will be described in details in the analysis section.

Fraud can also be grouped into 3 streams according to [17]; they are technical fraud (boxing, clip-on fraud, payphones, telecard fraud), not so technical fraud (calling card fraud, premium rate service fraud, subscription fraud), and not-technical fraud (audio text scams, comfort services abuse, cramming, PABX-hacking, slamming, social engineering).

Fraud has a negative impact on everyone, including residential and commercial customers. The losses increase the communications carriers operating costs [14]. In recent times, new fraud types and methods have emerged, and there is the need for practitioners in the field of telecommunications to update their knowledge, and also understand the trend and the losses involved due to these fraud activities. This will inform managers of telcos as to the urgency in deploying fraud

management systems regardless of the cost involved. This work therefore, intends to come out with a detailed analysis of the global fraud trends based on the global fraud reports of the Communications Fraud Control Association (CFCA) from 2008 to 2017, to inform decision making.

2 MATERIALS AND METHODS

This work employs purely secondary data from Communications Fraud Control Association (CFCA). The global telecommunications fraud reports from CFCA are analyzed using descriptive statistics to bring out interesting trends and information about fraud types and methods. All the reports were retrieved from Google search engine.

3 RESULTS AND DISCUSSIONS

3.1 GLOBAL TELECOM REVENUE AND FRAUD % LOSS TRENDS FROM 2008 TO 2017

The following analyses are based on the data from CFCA spanning the years 2008 to 2017. From Figure 1 below, global telecom revenues have increased gradually from 2008 to 2017. This shows that the telecom sector is doing well in terms of revenues worldwide despite the worrying trend of fraud. Year 2008 suffered the greatest fraud loss of 3.54%. This percentage was reduced considerably to 1.9% in 2011 with an increase in revenue from 1.7 trillion to 2.1 trillion. In 2013 however, fraud loss shot up again, and since then has been reducing considerably. In other words, the downward trend of the fraud % loss was curtailed by the value of 2013. Complacency set in when in 2011 the fraud % loss was reduced considerably, and this might have contributed in the value shooting up in 2013. The awareness was once again rekindled after the poor performance in 2013, and this might have contributed in the downward trend since 2013.

Managers of Telcos must not relax in the fight against fraud, since fraudsters are on daily basis coming out with new ways of perpetrating fraud. Fraud % loss is calculated out of the total revenue for the particular year; that is the fraud loss divided by the revenue, and the result multiplied by 100.

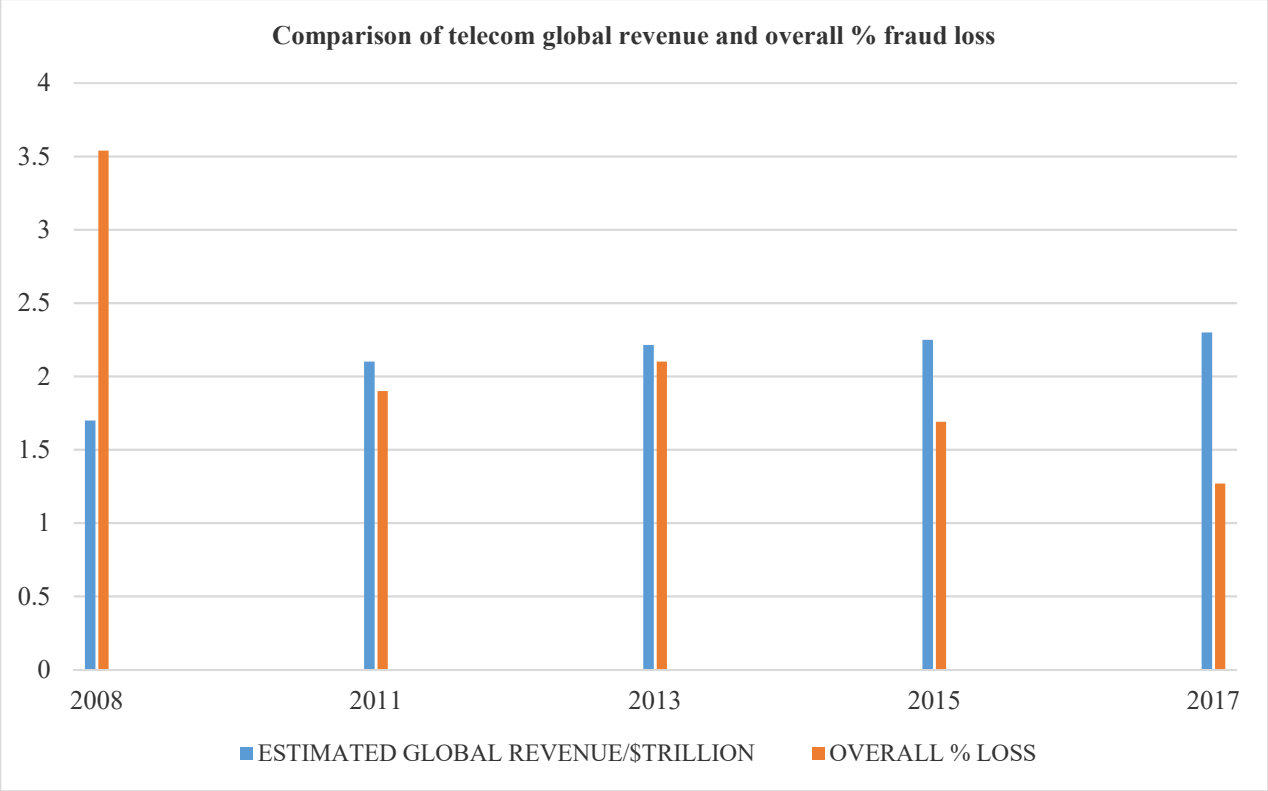

Fig. 1. Comparison of telecom global revenue and overall % fraud loss

Source: *CFCA*

3.2 GLOBAL TOP 5 FRAUD METHODS ANALYSIS

Table 1. Top 5 Fraud methods from 2008 to 2017

YEAR	METHOD OF FRAUD-TOP 5	% OF TOTAL LOSS (METHOD OF FRAUD)	REVENUE LOSS PER METHOD OF FRAUD/ $BILLION
2013	Subscription Fraud	11.3	5.22
	PBX Hacking	9.5	4.42
	Account Take Over / Identity Theft	7.8	3.62
	VoIP Hacking	7.8	3.62
	Dealer Fraud	7.2	3.35
2015	PBX Hacking	10.31	3.93
	IP PBX Hacking	9.27	3.53
	Subscription Fraud (Application)	9.27	3.53
	Dealer Fraud	8.24	3.14
	Subscription Fraud (Identity)	6.69	2.55
2017	Subscription Fraud (Identity)	6.95	2.03
	PBX Hacking	6.64	1.94
	IP PBX Hacking	6.64	1.94
	Subscription Fraud (Application)	6.61	1.93
	Subscription Fraud (Credit Muling/Proxy)	5.99	1.75

Source: *CFCA*

Until 2013, CFCA considered every form of fraud as fraud type. The separation into fraud type and fraud method happened in 2013 report. That explains the gap for 2008 and 2011 in table 1 above. From table 1, we realize that PBX hacking and Subscription fraud appeared for all the years in the top 5 fraud methods. Again, from table 1, from 2013 to 2017, subscription fraud recorded the highest percentage loss to fraud by 11.3%, followed by PBX hacking of 10.31% in 2015, and then PBX hacking of 9.5% in 2013. This means that they are really problematic areas which must be looked at critically. Regardless of the many controls in place, Subscription fraud is still venomous and prevalent [15]. The effect of subscription fraud does not stop with income loss alone. The impacts could be cataclysmic as far as escalating complaints, poor client or consumer experience, disappointment among support staff, and reducing investor confidence [15]. This is what [15] has to say about subscription fraud generally:

> "Subscription fraud is characterized by a fraudster using own, stolen or fabricated identity to get services with no intention to pay. The theft here is plain and simple but hard to detect 'intent' at the point of sale. The motive might be no more than being opportunistic or attempting to exploit a known vulnerability. However, this is now run by organized criminals – building multiple fraudulent identities over long periods. Furthermore, fraudsters have gained detailed fraud system knowledge and continually test the thresholds to exploit the loopholes in the systems. They even go as far as placing and grooming insiders to exploit the internal fraud systems. One interesting aspect of subscription fraud is that it's often classified as bad debt rather than fraud. The modus operandi goes something like – customer acquires services – the customer fails to pay – amount written off if unable to recover monies owed – reported as bad debt – the customer comes back again with a different identity and carries on as above. "

Private Branch Exchanges (PBX) are Telephone set ups utilized by little and medium organizations for inner and outer correspondences. They are as often as possible focused by culprits who misuse the innovation by committing what is known as PBX fraud (otherwise called 'dial-through fraud') – where the PBX is hacked into enabling calls to be steered through the system or set up to high rate international/premium rate numbers [16]. [13] also describes Private Branch Exchange (PBX) as a private telephone network used within a company. Acquiring a separate line for each employee in a company can be very costly, and so a PBX system switches calls between users on local lines while enabling them to share several external phone lines for making calls outside of the PBX. Three or four digit extensions are employed for calls within the company. The term PBX was first introduced in the time of switchboards, where operators would manually connect calls but over time, the process has become standardized. Private Branch Exchange (PBX) is a computer based switch that can be thought of as a small in-house telephone company [17]. This is what [16] has to say about how the fraudsters go about PBX hacking:

> "Once an auto-dialer has been used to identify systems which are worth hacking, the criminal attacks the system in order to establish the pass code that will give them access to the PBX system itself. Features such as remote-access

> voicemail, message forwarding and call diversion can all be exploited to enable the illicit call dialing. In the case of voice over IP (VOIP) telephony, systems are generally compromised by malware or accessing an IP address connected with the PBX box to bypass the company's firewalls."

[13] also describes the action of PBX fraudsters as follow:

> "PBX hacking happens when the networks don't have strong security systems. Hackers can penetrate weak PBX systems by direct inward system access (DISA) to make international, long distance, or premium rate phone calls. They can also listen to voicemails and phone conversations, change the call routing configurations and passwords, delete or add extensions, or even shut down the PBX entirely."

Some of the threats that affect PBX are theft of service, data modification, unauthorized access, disclosure of information, denial of service, and traffic analysis [17]. Also PBX threats result in loss of confidential information from voice mail, toll fraud, monitoring of calls, data modification, denial of service, rerouting of calls and impersonation, monitoring of room audio, and use of voice mailboxes which are not assigned [17]. From table 1, in 2013 alone, subscription fraud accounted for 11.3% of the total loss and PBX hacking fraud, 9.5%. In 2015 and 2017 however, subscription fraud was categorized into Identity, Application and Credit muling. In the case of identity theft subscription fraud, it is most of the time problematic for the casualty to determine the fraud as he or she may not find it for quite a while because of the idea of month to month telephone bills [13]. The inescapable nature of subscription fraud is due to the fact that it opens avenues to many different types of mobile fraud. Roaming fraud as an example, is as a result of scammers gaining access to a phone line through subscription fraud to accumulate charges on roaming networks [13].

For credit muling, this is what [18] has to say:

> "The practice of committing credit muling is simple: The fraudster convinces a person (the "mule" or "secret shopper", usually from a low social economical background) to provide him with high end mobile devices in return for a payment (usually a small amount, approx. $50-100) for each device this person provides. The "mule" is then instructed to sign a contract plan through one of the local telecom operators, then pay a small upfront payment and a minimum deposit and get a subsidized premium device. The device is then handed to the fraudster, leaving him with a high end mobile device that cost him couple of hundreds of dollars (and sometimes even less). From this moment on, the path to selling this device on the black market or abroad is very short. A simple calculation proves that after all out of pocket expenses, the fraudster still gains substantial profit of several hundred dollars for each device he sells, leaving the telco with invoices issued and sent to the mule, who is instructed to claim that he is a victim of ID theft fraud and not willing to pay the charges."

3.3 GLOBAL TOP 5 FRAUD TYPES ANALYSIS

From table 2, it is seen that premium rate service fraud has always been in the top 5 from 2008 except in 2011. This type of fraud directly attacks subscribers by getting them to make calls to a premium rate telephone number. Premium Rate Service Fraud happens when customers are ignorant of the additional charges linked to a call they have made [19]. This is what [20] has to say about premium rate service fraud:

> "Historically the vast majority, if not all, of the premium rate service (PRS) Fraud has been domestic (i.e. calls originating and terminating with the same country). The modus operandi is that fraudsters would acquire PRS numbers (e.g. chat lines, horoscope, news, gambling etc.) and inflate traffic to them with the knowledge that the telecom provider would pay them their 'revenue share' at the end of the month. As it takes a while for the operator to collect the money from the customer (usually at least 60 days), the elapsed time allowed the PRS fraudster to 'disappear' before being detected for fraud."

Again from table 2 it is seen that subscriber/identity (ID) theft was prevalent in 2008 and 2011 but did not show up in the top 5 for 2013, 2015, and 2017. Rather, lately, that is from 2011 to date, interconnect bypass fraud and International Revenue Share Fraud (IRSF) have become prevalent. The most common implementation of interconnect bypass fraud is known as simboxing. Enabled by VoIP GSM gateways (i.e., "simboxes"), simboxing connects incoming VoIP calls to local cellular voice network via a collection of SIM cards and cellular radios. Such calls appear to originate from a customer phone to the network provider and are transported at the subsidized domestic rate, free of international call tariffs. Interconnection bypass fraud negatively impacts availability, reliability and quality for legitimate consumers by creating network hotspots through the injection of huge volumes of tunneled calls into under provisioned cells, and costs operators over $2 Billion annually [21]. Bypass Fraud is used to describe the use of various least cost call termination techniques like SIM Boxes, Leakey (hacked) PBXs etc. to bypass the legal call interconnection and diverting international incoming calls to 'on' or 'off' network

UMTS/GSM/CDMA/Fixed calls through the use of VoIP or Satellite gateway, thus evading revenue for international call termination which operators and government regulators are entitled to [22]. Bypass fraud is a general term applied to many types of abuse involving the unauthorized re-routing of traffic in order to reduce interconnection costs, and thus either increase margins and/or attract customers by offering cheaper calls to [23]. The general term 'bypass fraud' includes many specific and well-known forms including; SIM-Boxes; Fixed Cellular Terminals (FCTs); Premicells; GSM/UMTS Gateways; Hedgehogs; Landing Fraud; VOIP Bypass; Interconnect Fraud; Toll Bypass; Third Country Fraud; Grey Routing; International Simple Resale (ISR). Over the past decade, bypass fraud has increased rapidly, leading to erosion in revenues of many fixed and mobile operators. Perhaps the commonest forms of bypass fraud today are: fixed to mobile bypass; international to national bypass; and PSTN to VOIP bypass.

IRSF initially, was committed by fraudsters by using SIM cards that are stolen or from subscription fraud to call international revenue share numbers either in roaming or international areas. The duration for processing call records was as much as 36 hours by the telco before the traffic would be terminated. During that window, fraudsters have the opportunity to dial as many international revenue share numbers as they could, producing huge dollars in benefits that the fraudsters would stash [13]. Now, due to technology, fraudsters rather inflate traffic to these international revenue share numbers. Attacks have therefore, become more systematized. To have multiple international revenue share numbers dialed into the same call and increase the cost, they employ for example, call forwarding and conference calling. Other innovations, for example, SIM cloning have turned into a critical danger. The rise of SMS spamming, PBX hacking, and Wangiri fraud have solidified IRSF as one of the greatest dangers in telecommunications fraud [13].

Table 2. Top 5 Fraud types from 2008 to 2017

YEAR	TYPE OF FRAUD- TOP 5	% OF TOTAL LOSS (TYPE OF FRAUD)	REVENUE LOSS PER TYPE OF FRAUD/$BILLION
2008	Subscription /Identity (ID) Theft	29	22
	Compromised PBX/Voicemail systems	20	15
	Premium Rate Service Fraud	6	4.5
	Hacking	4	3.2
	Arbitrage	4	3
2011	Compromised PBX/Voicemail systems	12.4	4.96
	Subscription /Identity (ID) Theft	10.8	4.32
	International Revenue Share Fraud (IRSF)	9.65	3.84
	By-Pass Fraud	7.2	2.88
	Credit Card Fraud	6	2.4
2013	Roaming Fraud	13.2	6.11
	Wholesale Fraud	11.5	5.32
	Premium Rate Service	10.2	4.73
	Cable or Satellite Signal Theft	7.7	3.55
	Hardware Reselling	6.4	2.96
2015	International Revenue Share Fraud (IRSF)	28.24	10.76
	Interconnect Bypass (e.g. SIM Box)	15.7	5.97
	Premium Rate Service	9.9	3.77
	Arbitrage	7.7	2.94
	Theft / Stolen Goods	7.45	2.84
2017	International Revenue Share Fraud (IRSF)	20.89	6.1
	Interconnect Bypass (e.g. SIM Box)	14.62	4.27
	Arbitrage	11.16	3.26
	Theft / Stolen Goods	10.34	3.02
	Premium Rate Service	8.18	2.39

Source: *CFCA*

4 CONCLUSION AND RECOMMENDATION

From the analysis done so far, subscription fraud as a fraud method tops all in terms of percentage loss from 2013 to 2017. The analysis revealed that the yearly global percentage fraud loss (calculated out of the yearly estimated revenue) was on the downward trend, with only 2013 being an abnormal case. Again, telecom revenues have been inching up gradually from 2008 to 2017. It was also revealed that PBX hacking and Subscription fraud appeared for all the years (2013 to 2017) in the top 5 fraud methods, and for fraud types, subscriber/identity (ID) theft was prevalent in 2008 and 2011 but did not show up in the top 5 for 2013, 2015, and 2017. Rather, lately, that is from 2011 to 2017, interconnect bypass fraud and International Revenue Share Fraud (IRSF) have become prevalent. Putting everything together, there are about five fraud types and methods that come to mind, which managers of telcos must pay particular attention to them to ensure considerable revenue recovery. These are Subscription Fraud, PBX Fraud, Subscriber/Identity (ID) theft, Interconnect Bypass Fraud (IRSF), and International Revenue Share Fraud.

ACKNOWLEDGEMENT

Special thanks go to Almighty God for granting ust he ability to come out with this work. Thanks also go to our colleagues and friends who in diverse ways helped me to finish this work.

REFERENCES

[1] P. Gosset, and M. Hyland, “Classification, Detection and Prosecution of Fraud on Mobile Networks”, n.d. Retrieved on 13022018 at http://www.chrismitchell.net/ASPeCT/CD%20Data/Papers/P31.PDF

[2] L. Cortesão, F. Martins, A. Rosa, and P. Carvalho, “Fraud Management Systems in Telecommunications: a practical approach”, n.d. Retrieved on 13022018 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.553.9706&rep=rep1&type=pdf

[3] H. Kvarnstrom, E. Lundin, and E. Jonsson, “Combining fraud and intrusion detection – meeting new requirements – In Proceedings of the 5th Nordic Workshop on Secure IT systems (NordSec2000)”, Reykjavik, Iceland, October 2000.

[4] Neustar, “WHAT THE FRAUD? A Look at Telecommunications Fraud and Its Impacts”, 2013.

[5] Nassau County Spin, “Telecommunications fraud”, n.d. Retrieved on 13022018 https://www.wantagh.li/spin/telecommunications_fraud.pdf

[6] M. Johnson, “Cause and effect of telecoms fraud. Telecommunication (International Edition)”, 30(12):80–84, 1996.

[7] A. B. Davis, and S. K. Goyal, “Management of cellular fraud: Knowledgebased detection, classification and prevention. In Proceedings of the 13th International Conference on Artificial Intelligence, Expert Systems and Natural Language”, Vol. 2, pages 155–164, Avignon, France, 1993.

[8] P. Hoath, “Telecoms fraud, the gory details. Computer Fraud and Security”, 20(1):10–14, 1998.

[9] H. A. E. Tawashi, “Detecting Fraud in Cellular Telephone Networks. Islamic University of Gaza Deanery of Graduate Studies Faculty of Commerce, Department of Business Administration”, 2010. Retrieved on 14/02/2018 http://library.iugaza.edu.ps/thesis/95684.pdf

[10] J. Hollmen, “User Profiling and Classification for Fraud Detection in Mobile Communication Networks. PhD thesis, Helsinki University of Technology, Department of Cognitive and Computer Science and Engineering”, Espoo, Finland, 2000.

[11] D. O’Shea, “Beating the bugs: Telecom fraud. Telephony”, 232(3):24, 1997.

[12] Apri, “if it sounds too good to be true-local prosecutors 'experience of fighting telecommunication fraud”, 2004, available:http://www.nadaaapri.org/pdf/sounds-tpp-good.pdf,[accessed on 26 October 2009]".

[13] I. Howells, V. Scharf-Katz, and P. Staple, “TELECOM FRAUD 101: Fraud Types, Fraud Methods, & Fraud Technology”, n.d. Retrieved on 14022018 at http://www.argyledata.com/files/Telecom-Fraud-101-eBook.pdf

[14] CFCA, “2009 Global Fraud Loss Survey”, 2009.

[15] SHANKAR, “Subscription Fraud – Control this and you can control your fraud losses”, 2014. Retrieved on 16/02/2018 http://frslabs.com/frsblog/2014/12/19/subscription-fraud-control-can-control-fraud-losses/

[16] Retrieved on 17/02/2018 at https://www.getsafeonline.org/software/PBX-fraud/

[17] D. Michaux (CEO Scanit), “Telecom Fraud”. Retrieved on 17022018 https://conference.hitb.org/hitbsecconf2007dubai/materials/D2%20-%20David%20Michaux%20-%20Telecom%20Fraud.pdf

[18] D. Eshet, “Credit Muling fraud”, 2014, filed in Business Analysis - #fraud management #cvidya #revenue assurance #marketing analytics #Revenue Analytics. Retrieved on 17022018 http://www.telcoprofessionals.com/blogs/33084/1039/credit-muling-fraud

[19] L. B. Childs, “Premium Rate Service Fraud”, 2014. Retrieved on 17022018 at https://www.fraudtechwire.com/premium-rate-service-fraud/
[20] Shankar, “Premium Rate Service Fraud and International Revenue Share Fraud – Note the difference to accurately detect and prevent them”, 2014. Retrieved on 17022018 at http://frslabs.com/frsblog/2014/11/26/premium-rate-service-fraud-international-revenue-share-fraud-note-difference-accurately-detect-prevent/
[21] COMMUNICATIONS FRAUD CONTROL ASSOCIATION (CFCA), “Global Fraud Loss Survey”, 2013. Retrieved on 18022018 at http://www.cvidya.com/ media/62059/global-fraud_loss_survey2013.pdf, 2013.
[22] SUBEX LIMITED, “White Paper Bypass Fraud- Are you getting it right?” n.d.
[23] SUBEX LIMITED. “White Paper Combatting the menace of Bypass Fraud”, n.d.