AJIT-e Academic Journal of Information Technology
10.5824/ajite.2023.04.003.x

2023 . Fall - Güz . Volume – Cilt: 14 . Issue – Sayı: 55

Regulatory Recommendations for Fraud Problem in The Turkish Telecommunication Sector*

Süleyman BAYRAM, *Başkent University, Department of Management Information Systems, sbayram12@gmail.com, 0000-0002-0969-3718*

Esma ERGÜNER ÖZKOÇ, *Başkent University, Department of Management Information Systems, Assoc. Prof., eeozkoc@baskent.edu.tr, 0000-0003-1728-5930*

ABSTRACT

Fraud has been a persistent issue throughout human history. As technology continues to advance in various fields, fraudulent activities adapt and evolve accordingly. The telecommunication industry, in particular, has undergone significant transformations since the early 2000s with the advent of mobile technologies. It is evident that telecommunication fraud has seen a substantial increase during this time, leading to serious financial and reputational damage. Therefore, combating and preventing fraud has become a crucial task in the telecommunication sector, as it is in all industries. This study delves into the topic of fraud, with a particular emphasis on telecommunication fraud. It investigates the experiences and efforts made to minimize and prevent fraud globally. Additionally, the study includes a focus group analysis involving two mobile operators in Turkey, aiming to understand the current situation and industry expectations concerning telecommunication fraud within the country. After evaluating the information gathered and examining the existing efforts, the study offers a series of regulatory recommendations for reducing and preventing fraud in the Turkish telecommunication sector.

Keywords **:** Fraud, Telecommunication, Regulation, CLI Spoofing

Türkiye Telekomünikasyon Sektöründe Sahtecilik Sorunu için Düzenleyici Öneriler

ÖZ

İnsanlık tarihinde süregelen sahtecilik sorunu, teknolojik alanlarda yaşanan önemli gelişmelerle birlikte farklı şekillerde karşımıza çıkmaktadır. Telekomünikasyon sektörü, 2000'li yılların başında mobil teknolojilerin yaygınlaşmasıyla büyük dönüşümler yaşamıştır. Bu süreçte telekomünikasyon sahteciliğinde de önemli artışlar yaşanmış ve ciddi maddi ve itibar kayıplarına neden olmuştur. Dolayısıyla tüm sektörlerde olduğu

* *This article is derived from Süleyman Bayram's master's thesis entitled " Türkiye Telekomünikasyon Sektöründe Sahtecilik Sorunu için Düzenleyici Öneriler", conducted under the supervision of Assoc. Prof. Esma ERGÜNER ÖZKOÇ.*

Araştırma Makalesi / Research Article
Date Received: 9.05.2023
Publishing Date: 22.11.2023

10.5824/ajite.2023.04.003.x

gibi telekomünikasyon alanında da sahtecilikle mücadele ve önleme çalışmaları büyük önem taşımaktadır. Bu çalışma, sahtecilik konusuna ve özellikle telekomünikasyon sahteciliğine odaklanarak, bu alandaki dünya genelinde yaşanan deneyimleri ve önleme çalışmalarını incelemektedir. Ayrıca, Türkiye'deki telekomünikasyon sahteciliği konusundaki mevcut durumu ve beklentileri anlamak amacıyla iki mobil operatörle yapılan odak grup çalışması da bu çalışmaya dahil edilmiştir. Toplanan bilgiler ve mevcut çalışmaların değerlendirmesi sonucunda, Türkiye telekomünikasyon sektöründe sahteciliği azaltmak ve önlemek için düzenleyici öneriler sunulmaktadır.

Anahtar Kelimeler **:** Sahtecilik, Telekomünikasyon, Düzenleme, CLI Manipülasyonu

INTRODUCTION

The fraud which comes from the Latin word "fraudem" meaning tendency to deceive, is defined by the Oxford Dictionary of Concise as criminal deception that uses false representations for unfair personal gain (Bolton & Hand, 2002; Becker et al., 2010). Fraud is a phenomenon that has always been experienced since the existence of humanity. Fraud gains new forms with every new technological step (Alraouji & Bramantoro, 2014). Fraud, which is usually carried out for financial gain, can sometimes serve for personal gains, political goals, or other objectives (Becker et al., 2010). Although it is known that fraud is used in many areas such as banking, telecommunications, finance, health, and academic processes, within the scope of this study, the problem of telecommunications fraud will be investigated, and various evaluations and suggestions will be given for Turkey.

About 5% of the annual revenue of telecommunications operators is lost due to fraud and this rate is increasing every passing year (Rebahi et al., 2014). In 2019, it was measured that there was approximately $ 28.3 billion in lost revenue due to fraud cases in the telecommunications industry worldwide (Communications Fraud Control Association, 2019). Telecommunication fraud is experienced in Turkey as well as all over the world and causes various losses. The total number of subscribers of mobile operators, which are the most important actors and major stakeholders of the Turkish telecommunications sector, is approximately 87 million and their annual net sales revenue is approximately $ 2,7 billion [6]. With fraud, not only loss of income, but also loss of reputation, customer satisfaction, number of subscribers, and various other losses can be experienced. Telecommunication is considered one of the most important sectors in terms of fraud as both operators and individual users are directly targeted (Alraouji & Bramantoro, 2014; Brown, 2005; Weiss, 2005; Abdallah et al., 2016).

1. LITERATURE RESEARCH

1.1. General Fraud Approach

It is possible to divide fraud into two types: internal and external. Internal fraud occurs when an employee makes an attempt against his company, which can be defind as either low

or high based on the employee's authority (Green & Choi, 1997; Beneish, 1997; Summers & Sweeney, 1998; Phua et al., 2010). External fraud, on the other hand, can occur in a broader spectrum, which can include customers, manufacturers, third-party thieves, and more.

In the twentieth century, fraud has increased considerably in sectors that require transactions and interactions. In many technological systems such as telecommunication networks, mobile communication, banking, and e-commerce, fraudulent activities cause significant losses. In the context of fraud, sometimes a method can be used only as a tool, and the main target can be a different sector. In other words, there may be cases of fraud intricately intertwined with each other. For example, fraudsters who want to commit credit card or banking fraud can send a text message or make a call to the person concerned. In this case, it can be said that both telecommunication fraud and banking fraud are present here since telecommunication tools are used. The fight between scammers and affected companies continues on an ongoing basis (Alraouji & Bramantoro, 2014). Various fraud management systems are available to detect, intercept and prevent fraud (Kou et al., 2004). Since fraud prevention describes stopping fraud before it happens, this is unlikely to be 100% achieved in real life (Bolton & Hand, 2022). Fraud detection, on the other hand, refers to the detection after the incident occurs. It is important to consider fraud detection as constantly evolving.

1.2. Telecommunications Fraud

When analog telecommunications networks were first used, there were various security vulnerabilities, and these led to simple fraudulent methods. Beginning with Joe Engressia, one of the famous fraudsters of the early period, realizing that he could control automatic call forwarding when he whistled at certain frequencies in 1957, and later with other methods developed, the fraudsters created devices to penetrate telephone systems and were able to provide free service for users by charging the operators completely (Becker et al., 2010). Later on, analog technologies left their place for digital technologies and so, did the nature of fraud (Pourhabibi et al., 2020). Even though it is possible to talk about many fraud methods and scenarios, telecommunication fraud can be grouped into 4 categories. Contractual fraud; aims to benefit from the services without paying a fee, hacking; aims illegal takeover of telecommunications networks and services, technical; aims to exploit weaknesses in mobile system technologies and requires high technical capacity and procedural fraud; illegal attempt against procedures implemented in systems to reduce the risks of fraudulent activities (Gosset & Hyland, 1999; Sahin, 2007). More than 200 types of fraud fall under these classifications in the telecommunications industry. The most important of them are subscription, superimposed, premium rate, roaming, and simbox fraud (Cortesão et al., n.d.; Kuşaksızoğlu, 2006; Farvaresh & Sepehri, 2011; Mohd Yusoff et al., 2013; Abdallah et al., 2016). The most common fraud methods among European Conference of Postal and Telecommunications Administrations (CEPT) countries are; CLI spoofing, PBX hacking, wangiri fraud, roaming fraud, call hijacking, and subscription fraud (Electronic Communications Services, 2018). CLI spoofing, one of the fraud types mentioned above, is encountered very seriously, can cause serious problems and income losses. The origin of the call is shown differently by manipulating the CLI to avoid high termination fees. In this way, much lower termination fees can be paid. This situation causes significant revenue losses for many operators. Regulatory institutions in the United States of America (USA) and Europe make many regulations and impose various sanctions on this issue. The interoperability of these different solutions in

10.5824/ajite.2023.04.003.x

terms of international traffic also poses a significant challenge, as these regulations differ significantly among countries. In this regard, the cooperation of all stakeholders, especially in the international sense, is extremely important (i3Forum, 2020).

1.3. Fraud Problem in Turkey

As in the rest of the world, the telecommunication sector in Turkey is developing rapidly and is opening up to new areas every day. However, some revenue and prestige losses can occur due to fraud, and this causes severe problems. Many of the problems and losses in the world related to fraud methods are also experienced in Turkey in the same and/or similar forms.

Information and Communication Technologies Authority (BTK) is the authorized body for regulation and supervision of the electronic communication sector in Turkey. Operators serving in the sector are authorized by BTK. Operators are responsible to the BTK and related regulations for issues such as service delivery and problems encountered during service delivery. In this respect, it is obvious that it would not be reasonable in today's technology and conditions to leave the solution to fraud problems in the telecommunications sector only to the public authority and regulations. Considering that every stakeholder in the sector may be a part of the fraud, as stated above, it is considered that all stakeholders should take their share of responsibilities for a solution. With various regulations prepared by BTK, it is aimed to prevent fraud scenarios within the scope of CLI manipulation within the framework of the legislation, and applications for these regulations are continuing actively. However, fraud problems continue to occur. At this point, in the examination carried out within the scope of Turkey's legislation, it has been observed that there is no special regulation regarding the precautions that operators should take against fraud and how the issue is generally approached. Thus, it is thought that there is a regulation gap in this area.

Subscription frauds, CLI spoofing, international call fraud, value-added service fraud, spam messages, and artificial traffic generation are the most common fraud types in Turkey. However, in this study, although telecommunication fraud and many scenarios are discussed in general, problems and solutions within the scope of CLI spoofing will be mainly examined. Because this problem has been increasing both in the world and in Turkey recently and causes significant revenue losses. There are disagreements in this context, particularly among operators in Turkey, and there is no useful solution currently implemented.

CLI spoofing scenarios in Turkey are generally realized by changing the CLI of calls originating from abroad and showing them as domestic calls. At this point, the main problem is that it cannot be determined precisely on the legal basis of who committed the fraud. When mobile operators detect a CLI spoofing case with their technical means, they first send requests such as closing the number to the fixed operators who delivered the call. These numbers are closed to services from time to time by fixed operators. Sometimes it is stated that even if fraud has been done, they are not aware of it and there is no action they can take at that point. In addition, since there is no distinction between operators in the sector according to the relevant legislation, it is stated that the requests within the scope of fraud should be delivered by the public authority, not by another operator.

There are some methods for detecting CLI spoofing. It is also known that these methods are used by mobile operators in Turkey. However, fraud detections made by the operators in the sector do not make much legal sense and it does not seem possible to impose sanctions within the scope of these detections. For this reason, the assembly of the experience of the actors in the sector and the administrative, technical, and legal power of the public authority seems to be essential for the solution of the problem.

1.4. Fraud Problem in World

According to the global telecommunications survey released in 2019 by the Communications Fraud Control Association (CFCA), the worldwide telecommunications industry revenue lost due to fraud at $28.3 billion in 2019 (Communications Fraud Control Association, 2019). The Global Leaders Forum's (GLF) report on actions to be taken against fraud in 2018 stated that fraudulent call traffic costs the international wholesale transit call industry approximately $17 billion annually (GLF, 2018).

A study was conducted by BEREC (The Body of European Regulators for Electronic Communications) in 2019 within the scope of fraud (CLI manipulation, Simbox, Wangiri, etc.) and misuse of E.164 numbers and the results were published in a report (BEREC, 2019). The survey was conducted with the public authorities of the countries in the telecommunications sector and 15 countries, not including Turkey, participated in the survey. As a result of this survey; it has been stated that there is a significant increase in fraud cases in countries recently, it is very important to act together as the whole sector for a solution, it would be beneficial to create a common fraud database and to publish this database and to prevent calls accordingly.

In 2022, a report was published by the ECC (Electronic Communications Committee) to review current regulatory practices from the perspective of various regulatory authorities to combat CLI spoofing (Electronic Communications Services, 2022). It was stated that some short-term solutions are already in use, but they are not usually real-time solutions. It has been argued that the regulatory authorities of CEPT countries, as well as organizations such as ITU (International Telecommunication Union) and BEREC, at both national and international levels, should encourage industry groups in the fight against CLI manipulation, such as information sharing and traffic analysis. In addition, it is stated that the use of proven techniques such as STIR (Secure Telephony Identity Revisited)/SHAKEN (Signature-based Handling of Asserted Information Using Tokens), which will be detailed later, maybe one of the long-term solutions in this context. However, it has been stated that it may be difficult to implement such techniques in the short term since they require a purely IP environment. In addition, it was stated that in the relevant countries, there is a blacklist of fraudulent numbers, operators are allowed to block calls if fraud is detected as technically possible, and procedures are developed to increase the accuracy and reliability of CLI, and cooperation studies were carried out between sector representatives and public authorities (Electronic Communications Services, 2022).

1.5. Preventive Measures Against Telecommunication Fraud

Many artificial intelligence solutions are offered against fraud as mentioned above. Most of these methods are carried out with the analyzes made on the call detail records (CDR).

10.5824/ajite.2023.04.003.x

However, there are some other long-term solutions to fight CLI spoofing (Electronic Communications Services, 2022). Some of them will be included in this section.

STIR/SHAKEN: It is based on the verified creation of all call ecosystem components. It consists of a centralized architecture that enables the parties initiating and ending the call to agree on verified information. It is currently implemented in the USA and Canada. It is expected that this method will evolve into a European-wide model shortly (i3Forum, 2019).

SOLID: SOLID (Social Linked Data) is a proposed set of contracts and tools for building decentralized applications based on linked data principles. This standard is built on HTTP (Hyper Text Transfer Protocol). With the authorization and encryption provided by the decentralized structure of SOLID, it is evaluated that it can be used for the verification of the caller number in the telecommunications ecosystem. SOLID has been evaluated together with STIR in terms of reducing international call fraud and it is thought that it can be used for flexible and secure communication between the same people. With this theoretical approach, fraud can be handled without any interruption to all stakeholders in the call flow. Although it has not been implemented by any operator yet, it is thought to be useful in theory (i3Forum, 2019; Sambra et al., 2016).

Blockchain: DLT (Distributed Ledger Technology) is a protocol that enables decentralized database management by multiple participants at multiple points (Yli-Huumo et al., 2016; Yaga et al., 2018). If implemented for numbering management, phone numbers can be used as digital assets. In addition, it will be possible for only certain actions to be performed by authorized participants and data to be exchanged securely and transparently (Electronic Communications Services, 2022). The use case where operators share information about subscribers' identity and certificates, the blockchain ecosystem that can be created between domestic and international operators, and the sharing of public key certificates to verify user identity are important features for the application of blockchain in this sector. In addition, various studies are carried out by organizations such as ITU on the use of DLT in telecommunication applications (International Telecommunication Union, 2019).

AB Handshake: AB Handshake is a method used to detect fraud in real-time based on cooperation between operators and to eliminate fraud within the group of operators by verifying traffic between networks. It has no direct link to a specific country or regulation and has emerged as a standalone solution. It is used for live traffic verification by operators located in different geographical areas. This method is offered by a private business initiative. It can be implemented in both IP-based and traditional systems and can be used without affecting networks and call flows. Since the numbering plans need to be shared to implement this method, integration, and coordination with the relevant regulatory authorities are required (GSMA, 2022).

2. RESEARCH METHOD

2.1. The Data Collection Method

The interview is one of the data collection techniques that allow understanding of people and relationships through verbal communication tools. In this study, a semi-structured

interview technique was used, and interviews were carried out with 2 of 3 mobile operators in Turkey. The relevant representatives of the operator who could not be interviewed were contacted and interview questions were conveyed to them. However, due to the privacy policies of the relevant operator, they abstained from participating in the interview.

The interviewed operators will hereinafter be referred to as the "X" and "Y" operators. Both operators have been serving in the sector since the early 2000s and they have significant experience in terms of both Turkey and the world telecommunication sector. According to the latest market data published by BTK, operators X and Y represent approximately 70% of the mobile market. An interview was held with operator X on 16.06.2021 and with operator Y on 30.06.2021. Interviews were held online with the participation of the operators' fraud team manager and experienced personnel, and with focus groups consisting of three-person teams. All the participants are highly competent and highly experienced people who have been working in this sector and in fraud issues for at least 10 years (Bilgi Teknolojileri ve İletişim Kurumu, 2022).

2.2. Interview Notes and Analyses

Apart from the questions prepared before, other issues were also discussed from time to time during the interviews. For the interview questions, both operators also responded in writing. In addition to these written texts, the notes taken during the interview and interview records were also used for analysis and evaluation through the Nvivo program, which is used in qualitative research analysis. The codes generated as a result of the evaluations are as follows; *"CLI spoofing, simbox, fixed operator, international call, national call, CDR analysis, test calls, legislation, wangiri, IRSF, A number, B number, machine learning, fraud systems, big data, AI, automation, manpower, dealer fraud, subscriber, false documents, SMS, M2M, bypass fraud, high income, artificial traffic, interoperability, audit, legislative regulation, common ground, revenue loss, social engineering, roaming fraud, simswap fraud"*.

In response to questions about which types of fraud are encountered in the sector and which types of fraud have been seen more frequently in the last 5 years; it was stated that CLI manipulation, simbox, wangiri, IRSF, and subscriber frauds were prominent, and it was also stated that fraudulent activities, although not very intense, occurred in value-added services, M2M (machine-to-machine) and social engineering.

In response to questions about what kind of fraud is experienced in voice traffic, what measures are taken for this, and how the CLI spoofing is detected; they noted that wangiri, bypass (simbox and CLI spoofing), and IRSF fraud. In addition, it is stated that CDR analysis and test call methods are used extensively for the detection and prevention of CLI spoofing. In addition, it was overemphasized that the problem is a situation between the actors in the operator ecosystem, and in this sense, the role of the BTK in terms of solution will be important. It was stated that it would be beneficial to carry out detailed inspections and investigations specific to the operators experiencing the problem and to use detection and analysis methods within the body of the BTK or through a mechanism that would involve the BTK and be equidistant to everyone.

In response to questions about systems used to prevent fraud and lost revenue in the last 5 years; the X operator said that the work continues on the transition to a new system

originating abroad and on the other hand, the Y operator indicated that the majority of the systems are provided by internal resources and also differentiated and customized systems are used for various methods such as CLI manipulation and simbox. It was remarked by both operators that the systems are significantly reliable thanks to intelligent systems such as artificial intelligence. X operator said that the cost of the fraud system to be established by an operator with 20-30 million subscribers is approximately $ 2-3 million, although it is not an official value. In addition, X operator stated that annual revenue losses due to fraud will not be less than $ one million. On the other hand, Y operator remarked that the loss of revenue due to fraud, which may occur in the range of $ 3-5 million per year, is prevented by their companies, and that annual revenue loss due to subscription and fake documents are estimated to be around $ 1,5-2 million.

In response to questions about which fraud scenarios are predicted to be encountered more in the future and whether they plan to reduce the impact of the human factor by using tools such as artificial intelligence and machine learning to prevent fraud, both operators stated that social engineering-related fraud cases are expected to increase further in the future. In addition, X operator said that SMS phishing methods and Y operator said that CLI manipulation and malware attacks carried out over smartphones and simbox may increase in the coming period. However, it was stated by both operators that methods such as artificial intelligence and machine learning were used significantly to prevent fraud. In addition, it was stated that robotic automation processes are increased, and maximum efficiency is tried to be obtained from human power. X operator indicated that the use of artificial intelligence is currently around 5% and it is planned to increase this to around 20% in the future. Y operator said that special artificial intelligence solutions have been developed for some types of fraud and it is planned to increase the use of artificial intelligence in the future.

In response to questions about what kind of losses are experienced after fraud and what are the technical, administrative, and legal expectations from the BTK in terms of preventing fraud, it was stated that the most significant loss was in revenue, and it is planned to increase the use of automation and artificial intelligence systems to reduce this. In addition, the issues shared by both operators are increasing the controls on fixed operators especially for CLI spoofing, imposing heavy sanctions against fixed operators who cause or commit fraud, and creating a common ground where operators and BTK can act together, it is necessary to making legal regulations and fighting against fraud together in this way. In addition, both operators stated that although they take many precautions against fraud, it is not possible to completely prevent it, but if they act together as an ecosystem, it can be prevented significantly. Lastly, in response to the question about whether there are reports or publications on fraud, both operators replied that there was no such report or publication officially.

2.3. Summary of Interviews

In the interviews, the perspectives of the sector representatives were seen in detail, both within the framework of the questions asked and in general on issues related to fraud. It is thought that there is an important solution expectation for the problem experienced

particularly in CLI spoofing. At this point, a common solution involving all the stakeholders of the sector is considered vital.

3. ASSESSMENT AND RECOMMENDATIONS

3.1. Model Proposal

The problems experienced in Turkey regarding CLI spoofing have been given in detail in the previous sections. Considering in light of the determinations and precautions made by the interviewed operators in their systems, it would be beneficial to look at this issue first at the solution point, since the main problem at this point is that the operators try to solve the problem among themselves. In this respect, the establishment of a fraud management system within the regulatory public authority of the sector, specific to CLI spoofing and other possible frauds will be beneficial. Operators should also be involved in this system. Some framework issues regarding how this system should be are as follows; call data of all operators will be continuously transferred to this system and as a result of detailed analyzes performed here, fraudulent calls and numbers will be detected. It should be ensured that the test call method, which is currently implemented by the operators, is also automated with the structures established on this system, and thus, the manipulation of calls, numbers, and operator flows should be determined. After the determinations are made, the data will be shared with the relevant stakeholders and sanctions may be applied to the operators who are found to be fraudulent. At this point, it is important that the system is transparent to each stakeholder and that the findings are presented to all stakeholders. Operators will both transfer data to the system and benefit from the outputs of this system. As a result of the activities carried out in the system, various administrative sanctions should be applied to the operators who are understood to have committed fraud, as specified in the relevant legislation, and measures should be taken up to the cancellation of the authorization of the relevant operator in case of the size or repetition of the fraud. Confidentiality of communication is essential in laws and regulations in Turkey. To avoid a process contrary to this principle, all information and data transmitted to the system must be anonymized. Moreover, to provide the legal infrastructure of the system, it is considered that a regulation that will include all the above-mentioned issues and that will specify the system architecture and the roles of all stakeholders should be implemented by the BTK Board. Thanks to this structure to be established, a collaborative ecosystem, as emphasized in the information obtained in the study, will be realized in real terms. The architectural structure that summarizes this system is given in Figure 1.

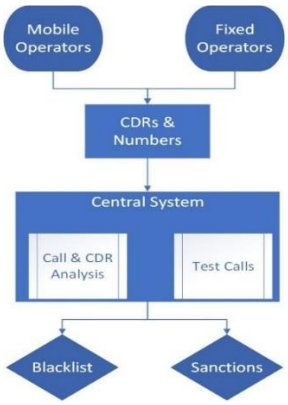

Figure 1: Central Fraud Detection System Architecture

10.5824/ajite.2023.04.003.x

3.2. Legislative/Regulative Proposals

It is thought that all transactions (subscription, number porting) involving physical document processes should also be carried out in digital environments, and thus, issues such as identity fraud will be prevented to a great extent.

While there are certain precautions and obligations regarding fraud in current regulations and practices, there is no special regulation directly targeting fraud in general. In this context, it is considered important that a Procedure and Principles titled "Measures to be Taken Against Fraud" is implemented by the BTK Board. The main issues that are considered to be included in these Procedures and Principles are as follows:

- All operators providing electronic communication services should take necessary measures against fraud in their networks and protect the subscriber.
- Operators should provide all the facilities for their subscribers to reach them and show maximum sensitivity to eliminate grievances.
- Operators should inspect their dealers regularly against fraudulent activities and must train dealers on countermeasures.
- Operators with more than ten thousand subscribers should establish a fraud team consisting of at least 3 experts in their field.
- Operators providing voice call services should take the necessary precautions in their network and prevent such calls within the framework of issues such as making too many simultaneous calls to a single number, simultaneous calls from a single number to many directions, and heavy traffic at certain numbers.

CONCLUSION

The main purpose of this study is to examine the cases of fraud in the Turkish telecommunication sector and to contribute to the measures that can be taken to reduce fraud. For this purpose, many important aspects of the subject have been revealed by conducting a literature review. Interviews were held with two mobile operators in Turkey with a market share of approximately 70% in total in the sector. The practices and measures taken within the scope of fraud in the world are included. Finally, in light of all this information, necessary discussions and evaluations were made and various suggestions were presented in terms of reducing telecommunication fraud in Turkey.

As a result of all the examinations and evaluations, a central fraud management system proposal, in which all stakeholders in the sector will participate, has been developed to prevent CLI spoofing. In this way, it is thought that the cases of fraud in this area will diminish significantly. In addition, it was stated that a regulation specific to fraud should be prepared and the basic framework of the said regulation was drawn. In this way, it is thought that a protective general framework will be drawn at both the operator and subscriber side and it will contribute to the reduction of fraud cases.

REFERENCES

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, *68*, 90-113. https://doi.org/10.1016/j.jnca.2016.04.007

Alraouji, Y., & Bramantoro, A. (2014). International call fraud detection systems and techniques. *Proceedings of the 6th International Conference on Management of Emergent Digital EcoSystems*, 159-166. https://doi.org/10.1145/2668260.2668272

Becker, R. A., Volinsky, C., & Wilks, A. R. (2010). Fraud detection in telecommunications: History and lessons learned. *Technometrics*, *52*(1), 20-33. https://www.jstor.org/stable/40586677

Beneish, M. D. (1997). Detecting GAAP violation: Implications for assessing earnings management among firms with extreme financial performance. *Journal of Accounting and Public Policy*, *16*(3), 271-309. https://doi.org/10.1016/S0278-4254(97)00023-9

Bilgi Teknolojileri ve İletişim Kurumu. (2022). *Elektronik Haberleşme Sektörü 3 Aylık Veriler Raporu 2022 – 1. Çeyrek*. https://www.btk.gov.tr/uploads/pages/pazar-verileri/uc-aylik-pazar-verileri-raporu-2022-1.pdf

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, *17*(3), 235-249. https://www.jstor.org/stable/3182781

Brown, S. (2005). *White Paper Telecommunication Fraud and Management.* Waveroad SecurIT,

Communications Fraud Control Association. (2019). *Communications Fraud Control Association Announces Results of 2019 Global Telecom Fraud Survey*. https://cfca.org/document/cfca-2019-fraud-loss-survey-pdf/

Cortesão, L., Martins , F., Rosa , A., & Carvalho , P. (n.d.). *Fraud Management Systems in Telecommunications: A practical approach*. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.553.9706&rep=rep1&type=pdf

Electronic Communications Services. (2018). *The role of E.164 numbers in international fraud and misuse of electronic communications services*. 2018. https://docdb.cept.org/download/1322

Electronic Communications Services. (2022). *CLI Spoofing. https://nkom.no/telefoni-og-telefonnummer/telefonsvindel/_/attachment/download/34a76b0e-011b-4bc0-b060-cc7761c0ffef:7b521945f6d348bd22fd3569e53458c8347fa51d/ECC%20Report%20338.pdf*

Farvaresh, H., & Sepehri, M. M. (2011). A data mining framework for detecting subscription fraud in telecommunication. *Engineering Applications of Artificial Intelligence*, *24*(1), 182-194. https://doi.org/10.1016/j.engappai.2010.05.009

GLF. (2018). *Taking action against fraud*.

Gosset, P., & Hyland, M. (1999). *Classification, Detection and Prosecution of Fraud on Mobile Networks*. http://www.chrismitchell.net/ASPeCT/CD%20Data/Papers/P31.PDF

Green, B. P., & Choi, J. H. (1997). Assessing the risk of management fraud through neural network technology. *Auditing : A Journal of Practice & Theory*, *16*(1), 14-28.

GSMA. (2021). *AB handshake global solution for call validation*. https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2021/04/AB-Handshake_whitepaper.pdf

International Telecommunication Union. (2019). *Technical Specification FG DLT D1.1: Distributed ledger technology terms and definitions*. https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf

i3Forum. (2019). *Calling line ıdentification (clı) management (release 1.0) june 2019*. https://i3forum.org/blog/2019/06/18/calling-line-identification-cli/

BEREC. (2019). *BEREC summary report on the Workshop on Fraud & Misuse of the E . 164 number range. https*://www.berec.europa.eu/sites/default/files/files/document_register_store/2019/12/BoR_%2819%29_241_-_Report_Fraud_Misuse_of_Numbers.pdf

i3Forum. (2020). *I3forum "calling line identification (Cli) spoofing" report*. https://i3forum.org/blog/2020/11/04/i3forum-calling-line-identification-cli-spoofing-report/

Kuşaksızoğlu, B. (2006). *Fraud detection in mobile communication networks using data mining* [Unpublished Master's Thesis]. The University of Bahçeşehir.

Mohd Yusoff, M. I., Mohamed, I., & Abu Bakar, M. R. (2013). Improved expectation maximization algorithm for gaussian mixed model using the kernel method. *Mathematical Problems in Engineering*, *2013*, 1-9. https://doi.org/10.1155/2013/757240

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). *A comprehensive survey of data mining-based fraud detection research*. https://doi.org/10.48550/ARXIV.1009.6119

Pourhabibi, T., Ong, K.-L., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems*, *133*, 113303. https://doi.org/10.1016/j.dss.2020.113303

Rebahi, Y., Thanh, T. Q., Busse, R., & Lorenz, P. (2014). On the use of unsupervised techniques for fraud detection in voip networks. In *Emerging Trends in ICT Security* (ss. 359-373). Elsevier. https://doi.org/10.1016/B978-0-12-411474-6.00022-0

Sahin, M. (2017). *Understanding Telephony Fraud as an Essential Step to Better Fight it* [Thesis]. École Doctorale Informatique, Télécommunication et Électronique, Paris.

Sambra, A.V., Mansour, E., Hawke, S., Zereba, M., Greco, N., Ghanem, A., Zagidulin, D., Aboulnaga, A., & Berners-Lee, T. (2016). *Solid :a platform for decentralized social applications based on linked data*. http://emansour.com/research/lusail/solid_protocols.pdf

Summers, S. L., & Sweeney, J. T. (1998). Fraudulently misstated financial statements and insider trading: An empirical analysis. *The Accounting Review*, *73*(1), 131-146. https://www.jstor.org/stable/248345

Weiss, G. M. (2005). Data mining in telecommunications. In O. Maimon & L. Rokach (Ed.), *Data Mining and Knowledge Discovery Handbook* (ss. 1189-1201). Springer-Verlag. https://doi.org/10.1007/0-387-25465-X_56

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview* (NIST IR 8202; s. NIST IR 8202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? —A systematic review. *PLOS ONE*, *11*(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Yufeng Kou, Chang-Tien Lu, Sirwongwattana, S., & Yo-Ping Huang. (2004). Survey of fraud detection techniques. *IEEE International Conference on Networking, Sensing and Control, 2004*, *2*, 749-754. https://doi.org/10.1109/ICNSC.2004.1297040