CENTRAL EUROPEAN UNIVERSITY

TACKLING FRAUD DISPUTES IN WHOLESALE TELECOM MARKET: WHAT CAN WE DO?

by Evgeniia Vasileva

Legal Department
Program: LLM in International Business Law
LLM Final Thesis
SUPERVISOR: Dr. Tommaso Soave
Central European University - Private University

Vienna, Austria
2021

Abstract

Telecommunications have become an integral part of our lives and now it is difficult to imagine the modern world without telephone calls, text messaging, and the internet. The wholesale telecom market is an important part of the global telecommunications market, which has its own features and issues. Telecom fraud is one of these issues.

First, this study investigates the reasons why the international traffic transit market is in such a vulnerable position for fraud. Subsequently, it examines the existing methods of fraud dispute resolution and critically assesses them. Finally, it suggests a way to tackle the issue of fraud disputes between the carriers.

A combination of normative and empirical research methods is used to conduct the research. An analysis of the contracts of mobile network operators and international wholesale carriers shows that only some companies include fraud provisions in the contracts. However, even these fraud provisions are quite general and do not cover procedural issues. To obtain the empirical data about the business practices of international carriers in dealing with fraud issues, an interview with the head of the disputes settlement department at a medium-sized international carrier was carried out.

The research results suggest that interconnection agreements can be the most efficient way to tackle the problem of fraud disputes. First, they are an integral part of the market since no company operates without signing a contract with its counterparty. Second, it would be possible to create a good business practice implementing the contracts. Third, establishing the fraud provisions in contracts allows the tackling of the problem of fraud disputes without changing the existing public law framework.

Table of Contents

List of Figures

List of Abbreviations

B2B	Business-to-Business
CDR	Call Detail Record
EDR	Event Data Record
FAS	False Answer Supervision
ITT	International Traffic Transit
MNO	Mobile Networks Operator
MVNO	Mobile Virtual Network Operator
NRA	National Regulatory Authority
PBX	Private Branch Exchange
QoS	Quality of Service
SMP	Significant Market Power
SMS	Short Messages Service
VoIP	Voice over Internet Protocol

Introduction

The international telecommunication market is constantly growing, becoming more and more important for the further globalization of the world. People are now looking for faster and better means of communications, and telecom companies are trying to meet this demand.

Nowadays, two individuals can easily communicate with each other even if they are in different countries or even different hemispheres of the Earth. Subscribers can connect among themselves by accessing the network of their mobile network operators (referred to as "MNOs" hereinafter). Telecommunication traffic flows from one MNO to another. However, it is not always a direct connection. In the process of its growth and development, the telecommunications market has evolved into a two-level system of retail and wholesale markets.

The business activity of MNOs is heavily regulated because of issues such as the protection of consumers and competition. In contrast, the activities of wholesale carriers remain a "grey area" for legal regulation. On the one hand, this creates a significant level of freedom for such carriers; on the other, it generates disorder in the industry.

International traffic transit includes companies of different sizes from different countries. One of the main features of the market is the interconnection between different wholesale carriers. Since carriers provide for traffic transit services, they need a connection with the networks of other companies to provide access to a greater number of destinations around the world. In some cases, traffic transit from point A to B requires the participation of a chain of wholesale carriers.

One of the most significant problems prevalent in the market is fraud. Generally, telecoms fraud is a crime involving the abuse of telecommunications services with the aim of stealing money from subscribers and/or telecommunications services providers. There are several types of telecoms fraud affecting the wholesale market including False Answer Supervision, call hijacking, software manipulation, etc.[1] All such types of fraud are digital crimes that can be committed from any part of the world where an Internet connection is available. Due to the transnational nature of the crime, there is usually little that law enforcement agencies can do to bring a fraudster to justice.

In these circumstances, telecom carriers have to regulate among themselves all issues related to fraudulent traffic. The carriers resolve such issues through fraud disputes between the chain's participants. The first dispute is raised between the telecom carrier who has initially detected the fraudulent traffic and its counterparty that sent the traffic. Later, corresponding disputes are raised between other carriers in the chain.

These disputes have a double aim. First of all, it is a signal that some portion of the telecom traffic was fraudulent and the payment for that traffic shall not reach the fraudster. Secondly, a fraud dispute is the way to settle money claims relating to fraudulent traffic. Once a fraud dispute arises between two carriers, a cascade of ensuing disputes will be raised among other carriers down the traffic chain.

This thesis will examine the reasons for the vulnerability of the international traffic transit market to fraud and critically appraise the existing regulatory frameworks for addressing the problem of fraud disputes. Since it is impossible to prevent acts of fraud, the thesis explores

[1] International Interconnection Forum for services over IP, 'Fraud Classification and Recommendations on Dispute Handling within the Wholesale Telecom Industry' (*I3FORUM*, May 2014). <http://i3forum.org/blog/2014/05/01/fraud-classification-and-recommendations-on-dispute-handling-within-the-wholesale-telecom-industry-release-3-0-may-2014/> accessed 12 January 2021

how the prompt resolution of fraud disputes, which is the consequence of the crime, can be facilitated. Considering the insufficiency of national and supranational legislation, the most effective way to address the problem is to include appropriate provisions in the relevant contracts among telecom carriers.

Even though fraud is a serious problem for the international wholesale telecom market, it has not yet been extensively investigated by scholars;[2] rather, this problem was addressed mainly in recommendations and codes of conduct of international forums specializing in telecom fraud. This thesis explores the way to respond to such a serious problem like fraud by means of private international law only and suggests recommendations that can contribute to the establishment of a self-regulatory system within the industry.

To achieve the aforementioned goals, a combination of normative and empirical research methods has been employed in the research project that took place at the office of LANCK Telecom, an international wholesale telecom carrier, between March 22 and March 30, 2021 (referred to as "LANCK Research Project" hereinafter). LANCK Research Project included two parts: (i) analysis of the contracts made between LANCK Telecom and several MNOs and wholesale carriers, (ii) interviewing the Head of Disputes Settlement department of LANCK Telecom. Information obtained during the LANCK Research Project served as an empirical basis for the thesis and helped identify the existing business practices in the industry related to issues of fraud.

[2] Scholars specialized in computer crimes mainly consider the problem from a forensic point of view and do not describe such a specific crime as telecoms fraud in the wholesale market. (See for example, C Walker, *Digital Evidence and Computer Crime: Forensic Science, Computers And The Internet*. (3rd edn, Academic Press 2011); I Walden, *Computer Crimes and Digital Investigations*. (2nd edn, Oxford University Press 2016). Researchers specializing in telecommunications law do not address this issue (see for example, I Walden, *Telecommunications Law And Regulation*. (5th edn, Oxford University Press 2018).

The first chapter of the thesis provides a general overview of the problem of fraud in the international traffic transit market. It describes the main features and principles of market operation, outlines the negative impact of fraud and fraud-related disputes between carriers, and highlights the existing regulatory approaches developed within the industry. This information serves as a background to understand the scope of the problem and discuss possible solutions.

The second chapter focuses more specifically on inter-company contracts as a key instrument for tackling fraud disputes. In the beginning, it provides an analysis of the place and role of contracts in the international traffic transit market. Then, based on the analysis of information obtained from the LANCK Research Project, this chapter highlights the existing business practices regarding provisions related to fraud and suggests recommendations on how a contract can be made an effective instrument in fraud disputes' resolution by including such provisions in the contract's special provisions: (i) liability for the network security, (ii) steps to take when fraudulent traffic is detected, and (iii) established dispute resolution procedure. The inclusion of these provisions in the contracts among all telecom carriers in the chain could speed up the resolution of fraud disputes. In turn, it would improve the chances to prevent fraudsters from stealing money, thus contributing to the fight against fraud.

Chapter 1. Challenges Related to Fraud in the International Wholesale Telecommunications Market

This chapter provides the necessary background to illustrate why telecom fraud is a huge problem for the industry and proposes the legal instrument to tackle fraud disputes between telecom carriers. Section 1 describes the structure and highlights the main principles of operation in the international wholesale market. Section 2 explains how fraud affects the industry and also discusses the reasons for the vulnerability of the market. Section 3 outlines the regulatory approaches developed by telecom carriers to tackle telecom fraud.

1.1 General Principles of Operation in the Wholesale Telecommunications Market

The telecommunications market a constantly growing together with technological progress. Therefore, it becomes more and more important for the further globalization of the world. People are now looking for faster and better means of communications, and telecom companies are trying to meet this demand.

Nowadays, two persons can easily communicate with each other even if they are in different countries or even different hemispheres of the Earth. Subscribers can connect among themselves by accessing the network of their mobile operators. Telecommunication traffic flows from one mobile network operator to another. However, it is not always a direct connection. In the process of its development, the telecommunications market has evolved into a two-level system: retail and wholesale.

The retail level consists of MNOs that provide telecommunications services to subscribers.[3] MNOs can be classified into two types of companies. Facility-based companies own networks and rely mainly on their own infrastructures to provide telecommunication services

[3] Ian Walden, *Telecommunications Law and Regulation,* (5th edn, Oxford University Press, 2018) 20.

to subscribers. Service-based companies (such as mobile virtual network operators [MVNOs]) do not have their networks and therefore lease access to the networks. The wholesale level appeared when facility-based companies started to provide wholesale services to service-based companies.[4] Subsequently, the market expanded with the emergence of facility-based companies that do not provide services to subscribers and are instead focused on B2B wholesale services for MNOs and MVNOs.

The wholesale telecommunications market, the main object of this thesis, offers a number of different services. Generally, they can be divided into the following categories: (i) services for accessing specific infrastructure owned or managed by MNOs; (ii) services for accessing the capacity of a network of MNOs; and (iii) services for the networks' interconnection and traffic exchange. This last type of wholesale services includes not only MNOs but also wholesale carriers – companies that do not have subscribers and provide traffic transit service to other carriers and operators. This thesis will examine this particular type of wholesale services, referred to as "international traffic transit" or "ITT" hereinafter.

An important feature of the ITT market is that it remains a "grey area" in legal terms. While the activities of MNOs are largely regulated by national authorities, wholesale carriers usually escape any strict regulation. The reason for this is that national regulation in many cases does not cover the cases when a telecom company: (i) do not have customers who are persons; (ii) do not have customers in the country of its incorporation; and (iii) operates

[4] Marc Bourreau, Johan Hombert, Jerome Pouyet and Nicolas Schutz, *Wholesale Markets in Telecommunications- CEPREMAP*, (June 2007) 2.

outside its country of incorporation.[5] This creates a significant degree of freedom for the companies, but it could generate disorder too.

Wholesale carriers and MNOs are interdependent participants in the market. Ideally, the exchange of traffic is carried out between two operators (see Figure 1 below).

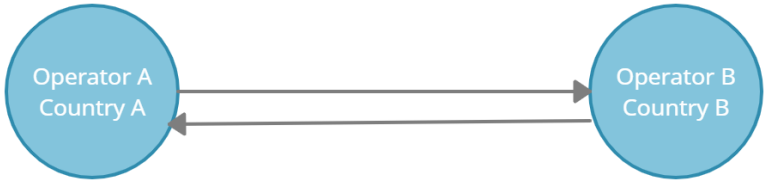

Figure 1: The exchange of traffic between two operators

However, it is not possible for an operator to have interconnection agreements with all other operators around the globe. For this reason, operators conclude the agreements with wholesale telecom carriers, who transfer traffic through their networks to different destinations of the world. Moreover, it is much more beneficial for the operator to conclude several agreements with wholesale carriers that already have interconnection agreements with a great number of operators than to get into individual contracts with each of them. Sometimes, telecom traffic is transferred through the networks of a chain of wholesale carriers to reach its final destination[6] (see Figure 2 below). Wholesale carriers have interconnections among themselves and with MNOs. It allows them to provide their customers with hundreds of destinations around the globe.

[5] This is provided in the national legislation of Cyprus, Bulgaria, and Hong Kong. Cyprus Electronic Communications and Postal Services Regulations Law 2004, N112 (I)/2004 of April 30, 2004 states that international traffic transit services are not licensed activities and therefore do not require authorization from the national regulatory authority. Bulgarian Electronic Communications Act (ECA) stipulates that a company does not need to submit a notification for the implementation of electronic communications services to the Communications Regulation Commission if the company does not intend to provide services within the territory of the Republic of Bulgaria. According to section 8(1) of the Telecommunications Ordinance of Hong Kong, only the provision of public telecommunications service is subject to licensing.

[6] Eric Johansson, 'Wholesale telecom Needs to Take Advantage of Digitalization Opportunities' *Verdict* (25 June 2020). <https://www.verdict.co.uk/telecom-wholesale> accessed 15 January 2021

Figure 2: The chain of telecom carriers

ITT constitutes a part of this global market, which is not so well-known outside the industry. Telecom traffic is transferred from one operator's networks through the wholesaler's network to the network of another operator. Payment for the service is calculated based on the amount of the transferred traffic. Companies involved in the transfer of telecom traffic form a chain. Telecom traffic travels from the beginning of the chain up to its end. Next, the companies in the chain issue invoices for the traffic received from each other. Each company pays its bill and issues the relevant invoice to its own customer that has sent the traffic. Eventually, the services of all companies in the chain are paid. Therefore, initially, the traffic goes down the chain and then the money flow follows. Companies rely on each other's good faith and pay the bills knowing that this amount will be compensated later by their client – another company in the chain.

Several types of telecom traffic can be transferred by wholesale carriers. In my paper, I will examine the following two sectors of the traffic transit market: Short Message Service (SMS) and Voice over Internet Protocol (VoIP). The technical side of the transfer of SMS and VoIP traffic is essential. Special computer software and hardware are integral parts of the whole process of the traffic transfer. However, this is one of the reasons for the vulnerability of this market to fraud.

1.2. Fraud in the Wholesale Telecom Market

Telecom fraud is a prevalent digital crime that is deeply embedded in the telecom market. For criminals, it is a low-risk financial crime, which causes a loss of €29 billion annually.[7] Telecom fraud develops alongside the telecom market and has become a fast-growing industry.

Technologies are constantly developing and telecom companies use them to make their networks bigger and better. However, the growth of the networks leads to their further automatization, leaving more room for their criminal use: "If a network becomes 10 times more scalable, then it could mean that attacks using that infrastructure will have 10 times the effect, damage, and cost."[8]Also, several factors contribute to the increase in telecom fraud such as reducing the costs of equipment suitable for network hacking and the availability of information on the Internet required to commit crimes.[9]

Professor Walden states that initially the idea to exploit networks to get free telephone service was driven by the curiosity of engineers.[10] Then, it was done by people to avoid expensive tariffs on long-distance and international calls.[11] Later, together with the further development and increased security of networks, telecom fraud has transformed from network manipulation to acts against subscribers.[12]

Some types of telecom fraud that target end users are known to most of the subscribers of mobile operators. For example, the Wangiri fraud or "one (ring) and cut" whereby the

[7] *OCCPR Report of March 2019*. <https://www.occrp.org/en/daily/9436-report-us-32-7-billion-lost-in-telecom-fraud-annually> accessed 23 January 2021.
[8] Trend Micro Research Europol's European Cybercrime Centre (EC3), *Cyber-Telecom Crime Report 2019.* <file:///D:/cyber-telecom_crime_report_2019_public.pdf> accessed 20 January 2021
[9] Ibid
[10] Ian Walden, *Computer Crimes and Digital Investigations* (2nd edn, Oxford University Press, 2016), 3 77.
[11] Ibid, 7 3.77.
[12] Ibid, 3.78.

fraudster generates thousands of calls to random phone numbers. After one or two rings, the fraudster drops the call, leaving a missed call on the subscriber's phone. Calling back, the subscriber hears a recording that serves to keep one on the line as long as possible,[13] Actually, the subscriber calls back on a premium rate number, which charges a much higher rate than a regular one.

Other types of telecom frauds like "False Answer Supervision" (FAS) are not so well-known. FAS is a type of VoIP fraud committed by a wholesaler in the carriers' chain. The fraudulent carrier returns a false answer signal to the earlier carriers in the chain and starts billing for the call. As a result, the billing starts before the distant customer actually picks up the phone and even when there is no reply from the other end. "International Revenue Share Fraud" can take several forms, such as fraudsters obtaining premium rate numbers and hacking the private branch exchange (PBX)[14] of a telecom carrier, or cloning SIM cards to generate artificial calls to these premium numbers. Other possible scenarios of fraud include software manipulation, call hijacking, numbers manipulation, etc.[15]

Telecoms fraud affects all participants in the market. Some types of fraud target only subscribers; others target subscribers and/or telecoms carriers, while some types of fraud only target telecoms carriers. Generally, telecoms fraud is reflected in the manipulation of either the origin or destination of the traffic to get payment before the fraudulent traffic can be disputed.[16] It must be noted that the type of fraud is not so important in the process of

[13] 'Fraud Classification and Recommendations on Dispute Handling within the Wholesale Telecom Industry'. <http://i3forum.org/blog/2014/05/01/fraud-classification-and-recommendations-on-dispute-handling-within-the-wholesale-telecom-industry-release-3-0-may-2014/> accessed 20 January 2021

[14] PBX is a telephone network within a telecom company that switches calls between users.

[15] 'Fraud Classification and Recommendations on Dispute Handling within the Wholesale Telecom Industry' (n 13)

[16] Global Leaders' Forum and Delta Partners, *Taking Action Against Fraud: Demonstrating the International Wholesale Industry's Leadership Against Telecoms Fraud* (October 2018) .9.

resolving dispute within the carriers' chain. The important information relates to the portion and origin of the fraudulent traffic.[17]

The effects of fraud on the ITT market is a largely unexplored area as existing studies on telecommunications law do not cover this topic. Moreover, instances of fraud in this market affects only telecom carriers. In many cases, companies tend to not disclose information about the committed crime since they do not want to demonstrate the weak protection of their networks.[18]

Fraudulent traffic is data that moves across the network with other traffic. For this reason, it is very difficult to tell fraud apart from regular traffic flows. Even special softwares cannot identify the fraudulent portion of the traffic with a 100% guarantee. At that stage, the traffic may be labelled only as suspected fraud.

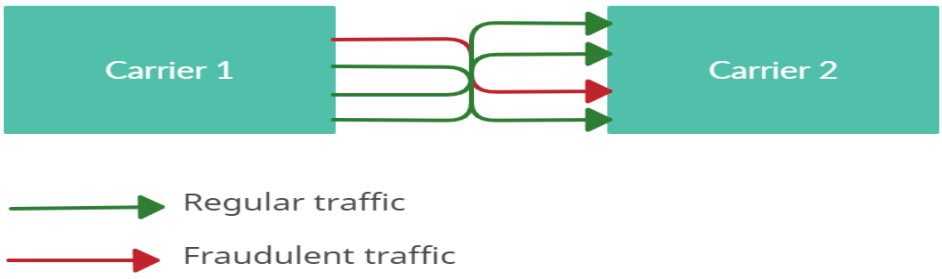

Figure 3: The flow of fraudulent traffic

<https://www.deltapartnersgroup.com/sites/default/files/GLF%20-%20Taking%20Action%20Against%20Fraud%20-%20October2018_0.pdf> accessed 20 January 2021

[17] LANCK Research Project.

[18] LANCK Research Project.

Therefore, fraud is usually detected much later, during the billing period. Telecom companies in the chain pay each other for the rendered service, i.e., the traffic transit. Each company issues invoices to its counterparts with the regularity established in the relevant contract. Usually, these periods are 7, 15 or 30 days long, depending on the billing policy of the company. Thus, the company that sent the traffic pays the invoice issued by another company that has "terminated"[19] it. All companies in the chain do it but not simultaneously because of the different billing periods. Wholesale carriers pay the bills and then issue their own invoices to their clients, expecting that the amount they have paid will be covered later by the payment of those invoices. Therefore, the mutual trust between the companies in the chain is an essential element of the market's functioning.

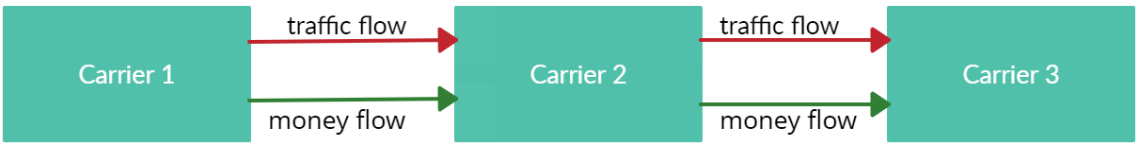

Figure 4: Traffic and money flows

What happens when fraud intervenes in these processes? If some portion of the traffic were fraudulent, the issued invoice will contain the amount due for the payment for this traffic too. The companies would then start to bill each other up to the beginning of the chain. Due to the different billing periods, some of those invoices might be paid before one of the companies detects inconsistency. The invoice amount may be significantly higher than the amount this company expects based on its internal information about the amount of the traffic that has been sent. In that case, the company initiates a fraud dispute with the billing company,

[19] "Termination" in the wholesale telecom market refers to the delivery of traffic to an endpoint, including the usage of networks of other carriers.

claiming to exclude the amount for the fraudulent traffic from the invoice. The corresponding disputes will be raised by other carriers in the chain. However, someone has to pay for this traffic. As a result of the fraud intervention, some company in the would not get any payment for its services. This situation may lead to the bankruptcy of small and medium-sized carriers. Meanwhile, bigger companies treat such losses as the cost of doing business.[20]

Despite the fact that fraud is a crime, in most cases, fraudsters avoid any responsibility.[21] One of the reasons for it is the international and sophisticated nature of the ITT market. While hacking a network located in a country, a fraudster may act from another country, and the company suffering the loss may be located in a third country. In such a case, local law enforcement authorities cannot arrest the citizens of another country. The level of the police's performance in governing the Internet is low and jurisdictionally based.[22] This is a common problem with crimes in cyberspace. Even when a national law imposes ex-post sanctions on Internet offenders, its actual efficiency remains questionable.[23] Moreover, in inter-jurisdictional cases, there is the problem of *nullum crimen* legal disparities, where an action is considered a crime in one jurisdiction but not in another. Furthermore, the severity of an offence could vary in each jurisdiction.[24]

Telecom fraud often originates usually in "developing and least-developed countries."[25] Because of a number of reasons, those countries do not provide the required assistance when dealing with international telecom fraud. In the absence of international collaboration, such

[20] Trend Micro Research Europol's European Cybercrime Centre (EC3*), Cyber-Telecom Crime Report 2019*. <file:///D:/cyber-telecom_crime_report_2019_public.pdf>accessed 27 January 2021
[21] LANCK Research Project.
[22] David S Wall, 'Policing Cybercrimes: Situating the Public Police in Networks of Security Within Cyberspace', [2007] 8(2) PPR 183–205 [DOI: 10.1080/15614260701377729].
[23] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999) 124.
[24] David S Wall, 'Policing Cybercrimes: Situating the Public Police in Networks of Security Within Cyberspace', [2007] 8(2) PPR 183–205 [DOI: 10.1080/15614260701377729].
[25] Trend Micro Research Europol's European Cybercrime Centre (EC3), *Cyber-Telecom Crime Report 2019*. <file:///D:/cyber-telecom_crime_report_2019_public.pdf>.accessed 27 January 2021

criminals can easily avoid being held liable for their crimes and effectively export telecoms fraud.[26]

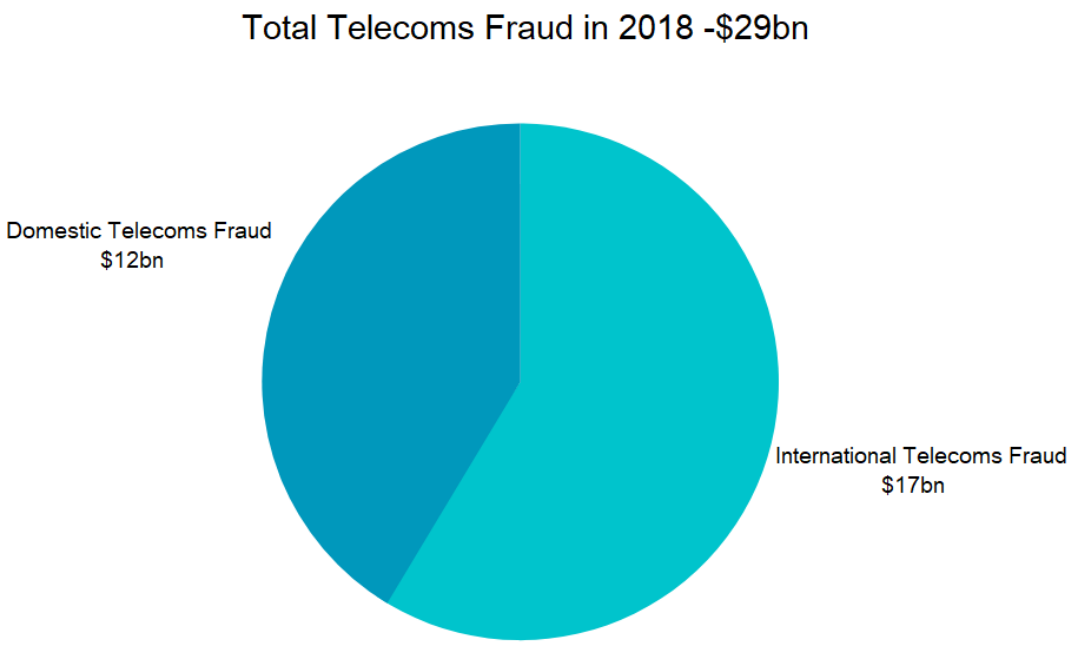

Figure 5: International Share of the Total Telecoms Fraud[27]

Another important aspect of the problem is that the investigation of telecom fraud crimes requires special technical equipment, time, and knowledge. Telecom fraud involves special features that distinguish it from other digital crimes and the daily public police agenda.[28] It affects the effectiveness of the police's ability to respond to these crimes.[29] Investigation may not only require technical skills and knowledge but also an understanding of the ITT market's

[26] Trend Micro Research Europol's European Cybercrime Centre (EC3), *Cyber-Telecom Crime Report 2019.* <file:///D:/cyber-telecom_crime_report_2019_public.pdf>.accessed 27 January 2021
[27] Global Leaders' Forum and Delta Partners, *Taking Action Against Fraud Demonstrating the International Wholesale Industry's Leadership Against Telecoms Fraud* (October 2018), <https://www.deltapartnersgroup.com/sites/default/files/GLF%20-%20Taking%20Action%20Against%20Fraud%20-%20October2018_0.pdf>accessed 20 January 2021
[28] David S Wall, 'Policing Cybercrimes: Situating the Public Police in Networks of Security Within Cyberspace', [2007] 8(2) PPR 183–205 [DOI: 10.1080/15614260701377729].
[29] Ibid 203.

functioning. Moreover, obtaining documents and other evidence may be very time-consuming because of the several participants in the carriers' chain.

Another problem is that cybercrimes like telecom fraud are characterized by small-impact victimisztions that are spread across different jurisdictions. In these circumstances, public police that are focused on local level issues cannot allocate sufficient resources to this type of crimes.[30]

The problem of the lack of required knowledge also arises if the telecom carriers decide to resolve a fraud dispute in court. The judges usually do not have a required understanding of the industry rules and practices, as well as the technical knowledge and expertise. To render a decision, a judge shall consider pieces of evidence, which consist mainly of specific documents such as as call detail record (CDR) or event data record (EDR). The examination of these documents may be very problematic for a person without the relevant experience. The same problem crops up if the parties refer their fraud dispute to arbitration. Even though in this case the parties are free to choose a competent arbitrator, it may be difficult to find one. Moreover, arbitration procedures are expensive and can last as long as civil litigation. As a result, some telecom carriers refer their disputes to independent experts outside traditional litigation or arbitration settings.[31]

Another important issue is that during the investigation of the fraud crime (which may take more than half a year), the amount in question remains "frozen." Even though the telecom carrier is obliged to pay for the fraudulent traffic, the local authorities can prohibit it until the

[30] David S Wall, 'Policing Cybercrimes: Situating the Public Police in Networks of Security Within Cyberspace', [2007] 8(2) PPR 183–205 [DOI: 10.1080/15614260701377729].
[31] LANCK Research Project.

investigation is completed.[32] Consequently, a service provider company in this scenario may not get payment for several months, although the fraudulent traffic was transferred long ago and the fraudster already got the money.[33]

To sum up, telecom fraud is a very attractive area for criminals because of the international nature of the market and technical complexity of the issue. For these reasons, fraud is regarded an integral part of the industry and is taken into account by the telecom carriers as a business risk. Considering the inefficiency of law enforcement authorities, telecom companies have developed different regulatory approaches to tackle fraud disputes.

1.3 Existing Industry Regulatory Approaches

As discussed previously, the investigation of telecom fraud is challenging for public authorities. In most cases, it is not possible either to find and arrest the fraudster or cover the damage. Hence, telecom carriers found themselves in a situation where the only way out was to find alternative ways to deal with the consequences of the crime.

Wholesale carriers have formulated some general rules to settle fraud-related disputes. Generally, there are three sources of these rules: (i) codes of conduct; (ii) business practices; and (iii) interconnection agreements amongst the carriers.

Usually, in the business world, a code of conduct (or code of ethics) may be defined as a set of ethical principles that govern the behavior of a company and dictates how employees should act. In some cases, the code may be used to expand the policies of a company according to the behavior of its counterparts. This is not a widely accepted practice and is only used by MNOs. They may include the code in a set of documents for signing while

[32] LANCK Research Project
[33] Ibid.

entering into a contract or add it as an annex thereto. Because of the prevailing bargaining power of the operators, wholesale carriers have no other option but to accept it as it is. By doing so, MNOs want to ensure that their counterparts follow the same principles and rules as theirs. Considering that the regulatory burden on operators is much bigger than on wholesalers, such precautions may be justified. The content of these codes is quite general and does not directly address the problem of telecoms fraud. For example, the code can include an obligation to conduct risk-based due diligence when selecting business partners, comply with all relevant laws, regulations, and standards in the countries in which carriers operate, and to combat fraud, theft, etc.[34]

Another possible option is codes developed by international forums and associations engaged in the telecom sector.[35] These codes may state more detailed and clear rules on how fraud and fraud disputes can be dealth with. Global Leaders' Forum's code of conduct, for example, establishes six principles for the prevention of fraudulent traffic: (i) carriers will include in their internal management reporting dashboards relevant metrics and targets for all top executives to understand, and oversee, all activity to reduce fraudulent traffic flows; (ii) carriers will adhere to the i3 Forum's recommended processes to detect and avoid fraud; (iii) carriers will actively monitor their individual traffic patterns to identify fraudulent number ranges and destinations; (iv) carriers will take all reasonable actions to avoid payment flows to the instigators of fraudulent traffic; (v) carriers will actively share information on

[34] LANCK Research Project.
[35] For example, i3forum, GSMA.

fraudulent traffic and its origination; and (vi) carriers will adopt the standard contracting terms addressing fraudulent traffic management.[36]

At the same time, the binding power of the codes is limited to the members of those forums and associations. Membership mainly interests bigger companies since they share the same principles as the other big players in the market and such membership is beneficial for their image and business reputation. Other companies may follow the rules provided in such codes but on a voluntary and non-binding basis.

Business practice is the oldest instrument to resolve fraud-related disputes. Wholesale carriers use the rules developed via practice to fill in the gaps of contracts. Business practice is always developing and changing depending on the current trends in the industry. The best practices of the industry are reflected in i3forum's "Fraud classification and recommendations on dispute handling within the wholesale telecom industry."[37] It offers general guidance on some important issues such as the responsibility of the parties (telecom carriers are responsible for securing their networks from exposure to fraudulent traffic/use and should be prepared to fulfill their financial responsibility toward downstream suppliers except when denying payment to fraudsters), which documents must be produced to confirm the fact of fraud ((i) CDR analysis; (ii) fraud description based on CDR analysis; (iii) official fraud letter from the operator; (iv) official document issued in the name of the customer company stating that the operator has not been paid or has incurred a loss (quantified) for the

[36] See Global Leaders' Forum, *Code of Conduct for International Carriers to Take Leadership in the Prevention of Fraudulent Traffic*.(2018) <http://i3forum.org/blog/2018/05/30/code-of-conduct-to-combat-fraud/> accessed 8 January 2021.

[37] i3forum is a non-profit industry body focused on promoting and enhancing collaboration among telecom carriers and developing the international carrier ecosystem. This organization addresses several problems within the industry, including telecoms fraud. At the moment, recommendations created by the i3forum's members are the most comprehensive source of information on telecoms fraud.

specific portion of traffic that is disputed, (v) police or other law enforcement authority reports), etc.[38]

However, there are two crucial disadvantages to using business practice as the main arbiter of disputes. The first is the absence of a binding power. Although a useful instrument, in practice, telecom carriers are not bound to follow the rules. The second disadvantage is the absence of practices common to the whole industry. Differences may originate from the legislation of the company's country of incorporation, or the area of the market where the company mostly operates.[39]

A contract is another source of rules for telecom carriers. Companies establish the main principles of their business relations in contracts and ensure that they are bound to obey it. Contracts are an integral part of the ITT market operation as every company signs an agreement with its counterpart. In some cases, this agreement shall be accepted by the other party without any significant change (as in the case of operators' contracts) or it is amended during negotiations.

In the ITT market, it is almost impossible to operate without having written agreements. Before sending traffic, the parties shall agree on several important questions including prices, billing method, and technical issues (such as the interconnection architecture and quality of service (QoS)).[40] These elements are essential for an interconnection agreement and are always included in its text. However, the very nature of the agreement allows significant flexibility with regard to additional conditions that may be included therein. The parties can expand the scope of their agreement by the inclusion of fraud-related provisions in the text

[38] Fraud Classification and Recommendations on Dispute Handling Within the Wholesale Telecom Industry. <http://i3forum.org/blog/2014/05/01/fraud-classification-and-recommendations-on-dispute-handling-within-the-wholesale-telecom-industry-release-3-0-may-2014/>accessed 21 Janiary 2021
[39] Such as North America, LATAM, MENA & South Asia, Europe, etc.
[40] LANCK Research Project.

and thus make them mandatory due to the binding nature of the contract. Moreover, in the absence of a unified regulation of the fraud issues in ITT market at the state level, private parties can address these issues in the international agreement amongst themselves.[41]

In these circumstances, a contract is a major instrument for providing legal certainty. A clear set of the parties' obligations contained in the contract is a pillar of contract law.[42] In particular, certainty about the obligations of the parties under the contract is especially important in situations where the particular issue is not regulated by law and the parties' respective intentions are uncertain. Therefore, a contract is the main source of the rules and principles for the ITT market, which does not enjoy legal regulation in most countries of the world.

All these factors make a contract the most promising instrument to tackle fraud disputes in the market. The parties can establish in contract not only some general principles but also procedural issues to make dispute resolution faster and more efficient. Moreover, the binding force of contracts and the chain structure of the ITT market can not only make rules mandatory for parties involved in a particular contract but also expand its effect on other carriers. A uniform set of rules established via contracts along the whole chain of carriers will contribute to the legal certainty and prompt resolution of fraud disputes.

[41] Souichirou Kozuka, 'The Economic Implications of Uniformity in Law. Uniform Law Review', (2007) 12(4) RDU, 686.
[42] Michael Greatrex, 'The Pursuit of Certainty: A New Approach to Best Endeavours Clauses.' (2019) 25 Auckland University Law Review, 155

Chapter 2. Contract as a Key Instrument to Tackle Fraud Disputes

International telecommunication traffic transit is a specific area that is not subject to national regulation in most countries of the world. In the absence of relevant public law, contracts take a dual role. First of all, they are binding documents between parties that define their mutual rights and duties. Secondly, they are the primary source of regulation, which shapes the internal rules of the industry. This chapter explores the function of contracts in the ITT market and their role in the regulation of fraud disputes. A detailed examination of contracts is carried out to assess whether they can be used as an effective legal instrument to tackle the problem. Section 1 outlines the general features of the international telecom traffic transit contracts. The current business practices in the regulation of fraud-related issues through special contract clauses are discussed in Section 2. The final section provides recommendations on fraud-related provisions to be included in the contracts.

2.1 The Importance of Contracts in the ITT Market

Contracts play a crucial role in the telecom market and are always integral to business relations. They are not only a written confirmation of the parties' arrangement but also a source of regulation including on significant technical aspects that are required to establish an interconnection. Thus, a contract always precedes the actual interconnection.

There are different types of telecommunications contracts, although two main categories are distinguished generally: (i) retail contracts, where one party is a telecoms network operator and the other is a consumer – natural person; (ii) wholesale contracts, where both parties are companies operating in the telecom market (usually telecom operators).[43] The second type of

[43] LANCK Research Project.

contracts can be divided into (a) contracts for the wholesale access to specific infrastructure,[44] (b) contracts for the capacity of a network[45], and (c) contracts that establish the interconnection of networks and exchanging (terminating or originating) traffic. The latter type of contract is called the interconnection agreement, and the parties involved in these agreements can be telecoms operators and wholesale telecom carriers. For the purpose of this paper, interconnection agreements are examined below.

There are many different names for interconnection agreements in the ITT market: interconnection agreement, telecommunication services agreement, bilateral (or unilateral) service agreement, reciprocal international voice (or SMS) agreement, etc.[46] Nonetheless, all these contracts have almost the same structural elements and identical provisions.

It must be noted that the conditions of interconnection agreements may vary depending on the parties thereto. Interconnection agreements among telecoms operators with significant market power (SMP) are more strictly regulated because of competition policy, which prevents SMP operators from abusing their position in the market.[47] One of the instruments of competition law is reference offers – standard contracts for access arrangements. National regulatory authorities (NRA)[48] may require SMP operators to publish their reference offers.[49] These offers were introduced as a remedy to ensure transparency and their conditions may be dictated by the NRAs. However, they are not considered public law documents but instead as private documents that must comply with public law requirements. The aim of reference

[44] For example, the local loop.
[45] Like Mobile Virtual Network Operator (MVNO).
[46] LANCK Research project.
[47] Ian Walden (ed), *Telecommunications Law and Regulation* (Oxford University Press, 2018) 535–8.
[48] In the EU, based on Article 67 (4) of Directive (EU) 2018/1972 (the EECC), the Body of European Regulators for Electronic Communications (BEREC) shall issue guidelines on the minimum criteria for a reference offer.
[49] Walden (ed) (n 47) 481.

offers is to prevent discrimination. So, any access seeker can claim that conditions of its agreement must be no less favorable than published ones.[50]

At the same time, interconnection agreements among wholesale carriers are not very regulated. They contain the same general provisions, including an interconnection architecture, planning, prices and billing, quality of service, etc. In contrast, there is a greater level of freedom and discretion for the parties involved.[51] Considering that the activities of wholesalers are not regulated in many countries, they have much more freedom in determining contract provisions than MNOs and SMP operators, who must comply with a large number of national legal regulations.

What makes a contract such a powerful regulatory instrument in the ITT market? As a rule, parties to an international contract choose the law to govern it. So, when some conditions are not established in the contract or when the interpretation of its provision is needed, the parties refer to the law of the chosen jurisdiction. However, this is not always a case for interconnection agreements.

Chapter 1 has already discussed the problem of regulation of the ITT market. It is significantly less regulated than the retail market, which operates mostly on a national level and thus has many governing legal sources, including competition laws. Furthermore, contracts with natural persons have additional sources of regulation in consumer protection legislation.[52] Therefore, if some matters are not directly mentioned in the contracts or are unclear, the relevant national legislation can fill in the gaps.

[50] Ian Walden (ed), *Telecommunications Law and Regulation* (Oxford University Press, 2018) 481.
[51] For example, in setting the rates or QoS.
[52] Walden (ed) (n 50) 491–4.

In contrast, the ITT market does not enjoy the same level of regulation. In most cases, wholesale carriers are not required to obtain authorization or license to conduct their business.[53] Moreover, national laws do not implement ex-ante sector-specific regulation of the traffic transit market, and the existing regulations for the retail market are not always applicable. Application for clarifications to NRAs can also be of limited use, given that their answer is based on national legislation.[54] In the absence of relevant laws, NRAs cannot provide guidance when the issue in question is not covered by the national laws.

In these circumstances, the role and importance of contracts in the ITT market becomes clear. It should be clear and detailed, because it may happen that there could be no appropriate source for gap-filling or interpretation. This is especially important for contracts with a wholesale carrier, which has a much higher level of freedom in setting the terms of contracts than SMP operators.

It is also important to highlight the role of contracts in the chain of carriers, which is a natural element of the ITT market. Each telecom carrier in a traffic chain is bound by an agreement with its counterparts. Contracts, therefore, regulate the relations of the whole chain of carriers. It is therefore a sensitive element for matters that can affect the whole chain such as fraud issues. For this reason, some provisions of the contract shall be drafted in line with the current business practices of the industry.

The formulation of business practices is another important role of contracts in the ITT market. In the absence of proper legislation, companies have to create an alternative source of regulation. Considering the high level of wholesale carriers' discretion in determining contract terms, business practice becomes a major source of different rules and principles.

[53] Ian Walden (ed), *Telecommunications Law and Regulation* (Oxford University Press, 2018), 288–9.
[54] LANCK Research project.

However, where can the companies find them? The most obvious source is a contract, wherein companies establish their obligations and rules on how particular issues shall be resolved. These provisions may certainly vary among MNOs and wholesale carriers, and companies of different size and from different countries. Nonetheless, some rules and principles can be found in almost any interconnection agreement[55] and form a "soft law" of the ITT market. Considering the importance of cooperation between the participants in a chain, it is essential to follow the relevant business practice, although it can be different with regard to particular issues. That is one of the reasons why some international companies have separate contracts for different types of counterparties and partners from different regions.

There is a special factor that explains the process of forming business practice in the ITT market. As mentioned in Chapter 1, there are different types of participants in the market. Some of them are MNOs, while others are wholesale carriers. The latter include companies of different sizes. Small and sometimes medium-sized carriers do not always have a lawyer, so they tend to simply copy the contracts of other companies, rather than drafting their own from the very beginning. In some cases, such borrowings are partial when different parts are taken from different contracts of other companies. In other cases, a company copies the contract of another company as a whole.[56] For example, at the very beginning of a company's activity, it usually incorporates the contract terms of bigger and more experienced counterparties.

This way, some rules and principles are tranferred to another company. Therefore, the business practice of the company will, to some extent, depend on the company wherefrom the original contract was taken. However, this does not mean that this practice could not be

[55] For example, the rule that each party to the agreement shall bear the cost of provision and maintenance of telecommunication facilities located within its network as well as that of the establishment and maintenance of one-half of the facilities necessary to provide service between the parties' networks.
[56] LANCK Research project.

changed in the future. The ITT market requires cooperation between companies. When provisions in the contract of a company differ significantly from the well-established practice of other companies, the provisions will always remain a matter of controversy. To avoid this, the company can follow another practice that is more common in the region of its main business activity. Therefore, companies influence each other through their contract texts and negotiations over contract provisions.

As a result, contracts play an essential role in the ITT market. It is a ground for establishing an interconnection among the parties' networks. In the absence of the relevant national legal regulation, they act as a statement of arrangement among the parties and as the main source of regulation for their business relations. Moreover, provisions of contracts form an essential part of the business practice of the ITT market. While some matters are covered by the common business practices within the industry, addressing other sensitive matters like fraud still lack a uniform approach.

2.2 Fraud-Related Provisions of Contracts

As discussed in Chapter 1, international transit of telecom traffic involves different types of companies. The first type is mobile networks operators including SMP operators. These companies provide services to subscribers and act as the originators of traffic. When a bilateral traffic exchange between the networks of two operators is not possible, the operators need to engage a wholesale carrier as an intermediary between the two networks.

While the business activity of mobile networks operators is heavily regulated on a national level, wholesale carriers enjoy much freedom. This difference is reflected in their contracts. Operators prefer to use long and detailed contracts, wherein they try to address all possible issues and scenarios. In contrast, wholesale carriers usually employ a much shorter and

simplified form of interconnection agreement. Consequently, the scope and content concerning fraud-related provisions in the contracts of operators and carriers vary.[57]

Generally, provisions pertaining to fraud are not an obligatory part of interconnection agreements, and at the very beginning, it does not seem to be as important as, for example, rates, list of destinations or QoS. Hence, interconnection agreements could be signed even in the absence of fraud-related provisions in the text. The absence of these provisions will only be noticed later when the first fraud dispute arises.

The importance of fraud-related provisions is well known to companies that face the problem of fraud on a daily basis and deal with a large amount of telecom traffic. Therefore, in most cases, fraud-related provisions may be found in the contracts of mobile networks operators, big wholesalers, or carriers that already have significant experience in the industry.

The following information is derived from the data obtained from the LANCK Research Project conducted at the office of LANCK Telecom, an international wholesale telecom carrier, between March 22 and March 30 in Saint Petersburg (Russia). Due to my prior employment there, the company granted me a short-term access to its database and files to conduct the research. The project included two parts: (i) analysis of contracts made between LANCK Telecom and several mobile networks operators and wholesale carriers, and (ii) interviewing the Head of Disputes Settlement department of LANCK Telecom. The combination of the knowledge obtained during both the stages of the LANCK Research Project enabled me to identify the existing business practices of the industry and prepare recommendations on fraud-related provisions to be included in contracts.

[57] LANCK Research project.

a) SMS Agreements

Regarding interconnection agreements for the transit of SMS traffic, fraud provisions are only included in the agreements of mobile networks operators, although are not very detailed. In most cases, fraud-related issues are mentioned in the following contexts:

1) General responsibilities of the parties – The parties undertake not to use the services for the transmission of unlawful, fraudulent, harassing, libellous, abusive, or otherwise objectionable content.

2) Liability – The parties exclude the application of limitation of liability clauses in the case of willful default or fraud. Each party obliges to compensate any loss or damage caused by fraud, gross negligence, or willful default of that party.

3) Termination or suspension – Either party may terminate or suspend the agreement in the case of fraudulent, unlawful, or unauthorized use of services by the other party, a third party, or users.

These fraud-related provisions not only address the actions of the third parties but also that of the parties to a contract, for which, there are two reasons: (i) due to the chain structure of the market, technically, it is one of the parties to the contract that sends the fraudulent traffic (the originating party) even when it has been received from the previous carrier in the chain; and (ii) the originating party can also be a participant in the fraud.

In most cases, such contracts do not contain a special section dedicated to fraud-related issues. Additionally, there is no clear guidance on procedure in case of fraudulent traffic's detection. However, some contracts dictate that one party may block the other from sending

unsolicited messages or fraudulent messages until the matter is resolved. Therefore, a procedural measure for blocking fraudulent SMS traffic is sometimes established in contracts.

Another problem is that the term "fraud" is used synonymously with "spam" in some contracts. Some SMS agreements explicitly provide in the "Definitions" section that "SPAM" or "SPAM message" shall mean any unsolicited or undesired SMS which is sent to users without their prior due consent and/or contains deliberately manipulated sender ID to bypass rules, commercial terms, or any other obligation, etc., and/or is fraudulent. In other contracts, these two terms are used together as "unsolicited and fraudulent traffic". Unfortunately, these contracts do not provide definitions that allow to distinguish spam and fraud. Therefore, in SMS agreements, the concept of "fraud" remains unclear.

To sum up, SMS Agreements do not ensure a sufficient level of regulation of fraud-related issues. In the absence of clear rules and procedures, fraud disputes tend to be time-consuming. Considering the importance of the prompt resolution of fraud disputes, this situation requires improvement. The confusion surrounding the terms "fraud" and "unsolicited traffic" (spam) makes dispute resolution even more problematic.

b) VoIP Agreements

At least 50% of interconnection agreements on the transfer of VoIP traffic drafted by wholesale carriers do not contain fraud-related provisions. Moreover, only 20% of the contracts without explicit fraud-related provisions include an obligation of the parties to protect the security of their networks.

With regard to the other 50% of interconnection agreements, fraud-related provisions are usually spread throughout the text of contracts. Only some contracts have a separate section

dedicated to fraudulent traffic. In most cases, these provisions are located in the following sections:

1) Liability – Each party shall be liable for the fraudulent and illegal use of the services by its subscribers/customers. The parties shall agree to work together to recover the payment for fraudulent calls.

2) Network security – The parties shall cooperate on all issues related to fraud, misuse, or damage of data and the network.

3) Termination or suspension – Each party may suspend and/or terminate the services and/or the agreement if a party reasonably suspects or proves fraud on the part of the other party in connection with the service.

4) Billing and payment – Each party shall be liable to pay for all the calls terminated by the other party at applicable rates, including, without limitation, calls that the originating party claims are fraudulent or otherwise un-billable, regardless of any bad debt, or other uncollectible amounts incurred by the originating party.

In short, fraud-related provisions in contracts emphasize the role of carriers' cooperation. This is important since the resolution of fraud disputes in the ITT market requires the active involvement of all carriers in the chain. Further, the level of parties' cooperation, in practice, determines the speed at which they can detect fraudulent traffic.[58] The sooner they can respond, the more likely the carriers are to prevent a fraudster from getting money.

[58] Global Leaders' Forum and Delta Partners, *Taking Action Against Fraud Demonstrating the International Wholesale Industry's Leadership Against Telecoms Fraud* (October 2018) < https://www.deltapartnersgroup.com/sites/default/files/GLF%20-%20Taking%20Action%20Against%20Fraud%20-%20October2018_0.pdf>accessed 17 March 2021

Regarding the last provision, it must be noted that the conditions concerning the payment for fraudulent traffic may vary. Some companies can expressly declare that they do not pay for any proven fraudulent traffic. Other companies follow a special disputes procedure for fraud claims. In some rare cases, wholesale carriers establish that they cannot prevent the fraudulent use of services and both parties shall be responsible to pay for all usage of the services including fraudulent usage. In fact, these companies refuse to raise disputes based on a claim or allegation of fraud. However, such indemnification is not a very popular approach in the industry.

Meanwhile, contracts of mobile networks operators include much more detailed provisions on fraudulent traffic. Around 40% of operators' contracts examined in the LANCK Research Project contained a special section about fraud. Usually, this section includes the following conditions:

1) General obligation to prevent and eliminate any kind of fraud or abuse that involves the parties' respective networks or services – Each party shall use reasonable efforts to monitor traffic to prevent and eliminate any kind of fraudulent traffic, abuse, misuse, or damage of data that involves the parties' respective network or services.

2) Indemnification – The originating party shall indemnify and hold the traffic transit service provider innocent of any such fraudulent or uncollectible use of services.

3) Payment for fraudulent traffic – The debtor party shall not be liable to make any payment to the creditor party for any bilateral traffic for which the debtor party has not yet been paid due to suspected fraudulent traffic.

In some countries, national legislation requires operators to include provisions regarding the payment for fraudulent traffic in their contracts. For example, the Latvian Electronic Communications Law[59] stipulates that "the interconnection contract shall provide for the procedures […] for mutual payments in cases when fraud performed using numbering or incorrect use of numbering is detected".[60]

Some contracts of operators comprise a detailed description about fraud disputes' regulation. For example, it can mention that the service provider will use reasonable efforts to obtain a credit note[61] from its service providers if the originating party presents all necessary information to prove the fraudulent nature of the traffic sent, including a CDR analysis, a detailed fraud description based on this analysis, the originating party's registered complaint to the local authorities, and other documents. These provisions can exclude the responsibility of the service provider for failure in obtaining a credit note from any of its counterparties. Fraud provisions can also force parties to cooperate and to try to stop the money flow to the downstream carrier in the chain.

Fraud-related provisions can be found in the "Termination" section where the fraudulent or abusive use of the services or even the absence of reasonable measures required to prevent such use may be a ground for the immediate termination of a contract. The "Liability" section, as a rule, excludes the limitation of either party's liability for fraud or willful misconduct.

[59] Before 2011, Latvia had the highest telecoms fraud rate in Europe. The scale of the problem was so significant that major international operators preferred to block Latvian numbers instead of trying to identify fraudulent calls. Later, Latvia became one of the first countries in the EU that introduced the term "fraud using numbering" and made serious amendments in its legislation to tackle the problem.
[60] Section 37(5) of the Electronic Communications Law of Latvia of 17.11.2004.
[61] Credit note is a document confirming that the cost of the fraudulent traffic has been credited by the service provider.

Another section of the VoIP agreements that can contain fraud-related provisions is the "Billing and Payment" section. It can stipulate that each party shall be solely responsible for the billing and collection of payments from its customers and shall bear their own risk with respect to fraud on their network. Moreover, these provisions can establish a time frame for raising a fraud dispute. In case of suspected fraudulent traffic, an invoice can be deemed accepted if the party discovering fraud does not raise the fraud dispute within the specified period.[62]

In most cases, fraud disputes are not allocated to a separate category. However, some operators establish special conditions for raising their disputes, such as a limited time frame, the list of documents to be provided, an opportunity to raise the dispute with other carriers in the chain successfully, and obtaining a credit note by the concerned party's service provider for the alleged fraudulent traffic. In addition, some operators stipulate a time frame to resolve the fraud dispute.[63]

Even though operators' contracts use the term "fraud," they usually do not define it. During the LANCK Research project, only one contract was identified wherein an attempt was made to define fraudulent traffic. In that contract, fraudulent traffic referred to (1) any calls and messages delivered by the originating party to the service provider for further routing, for which the originating party is unable to collect payment from its subscribers, customers, or business partners, or (2) sending, routing, or receiving messages, or making, routing, or receiving calls using the services, resulting in useless or artificial traffic, which may be expressed as uniform calls in the duration of a connection, or as calls or messages in an uncharacteristic amount for a user. In the discussed contract, the operator tried to provide a

[62] Usually, such a dispute shall be raised as soon as possible but not after the due date of the relevant invoice payment.
[63] 60 days, as a general rule.

comprehensive definition of what may be considered fraud in traffic transit. The GSMA's Fraud Manual provides a more general definition: "Fraud is perpetrated, where process, control or technical weaknesses are intentionally exploited, resulting in a financial or other loss."[64]

As mentioned in this manual, different countries apply a different definition of fraud, and operators may use different definitions within their businesses and countries.Fraud in telecommunications is a fast-growing area as new types and schemes of fraud appear constantly. This is why it may be an unsolicited practice to provide the definition of "fraud" in the contract. A detailed definition cannot cover all types of fraud, while a broad definition, as given by the manual, is not very useful.

To sum up, fraud-related provisions are used more often in VoIP agreements than in SMS.[65] For both types of agreements, MNOs lay down the most detailed and comprehensive regulation of fraudulent issues than wholesale carriers usually do. The concept of fraud in the SMS traffic transit market is still in the process of developing, which at the moment is considered synonymous with "spam." Most operators include fraud-related provisions in their contracts. In the contracts of wholesale carriers, the number of contracts containing these provisions is significantly lower as they do not face telecom fraud as often as operators and therefore are not very aware of the scope of the problem. Additonally, wholesale carriers usually have less bargaining power, so they try to exclude from their contacts provisions that can cause controversy. Provisions in operators' contracts demonstrate their level of expertise on issues of fraud. Operators clearly state the obligation to protect the safety of the parties' networks and define the responsibilities of the parties in case of fraudulent traffic's detection.

[64] GSM Association, *Fraud Manual*, version 16.0 (08 August 2018), 5.
[65] It may be explained by the fact that fraud in the SMS market is a relatively new concept.

Furthermore, the procedure for fraud disputes' resolution in many cases is thoughtful and detailed.

As discussed from this sub-chapter onward, there is a great variety of approaches to fraud-related provisions and their content, which causes certain problems when it comes to the resolution of fraud disputes in the ITT market. The establishment of some general rules and principles could greatly facilitate fraud dispute resolution.

2.3 Recommendations on Fraud-Related Contract Provisions

Contracts have the potential to become an effective instrument to tackle fraud disputes. Establishing certain rules and principles would make it possible to create uniform rules for fraud disputes' resolution. Some of these rules and principles already exist and are commonly used by big mobile operators.[66] These principles were created by specialists with significant experience in the industry and originate from the best business practices developed by the incumbent operators.

As mentioned previously in this chapter, contracts are the most effective instrument for the regulation of business relations' among carriers. Establishing a common set of rules regarding fraudulent traffic in a contract would be a step toward the creation of common business practices among wholesale carriers.

a) Liability For Network Security

The fundamental principle that should be established in an interconnection agreement is the liability for network security. Fraudulent traffic enters the chain through the network of one

[66] See for example, International Interconnection Forum for services over IP, *Fraud classification and recommendations on dispute handling within the wholesale telecom industry* <http://i3forum.org/blog/2014/05/01/fraud-classification-and-recommendations-on-dispute-handling-within-the-wholesale-telecom-industry-release-3-0-may-2014/>

of the participants. Therefore, the failure of one company to protect its network causes problems for the whole chain.

It seems unfair that a victim of a crime should compensate for the losses caused by the criminal. However, digital crimes now are deeply embedded in the market, and failure to protect the network is considered a violation of the company's obligations toward its clients and business partners. Therefore, although a fraudster may intervene in the company's network operation, the company's inability/failure to duly protect its network may contribute to the fraud being committed.

As explained in the previous chapter, in most cases, it is impossible to bring a fraudster to justice. However, the damage caused must be compensated. Other companies in the chain that have accepted the fraudulent traffic and forwarded it through their networks trusted their partner, supposing that it was regular traffic that will be paid. It may be argued that in these circumstances, each company should check the traffic that it receives from counterparties. In some cases, fraudulent traffic has specific features that allow its determination. However, these features are activated only when fraudulent traffic is generated. This type of traffic can be detected by special software that scans the traffic flows and analyzes them under particular criteria. Unfortunately, such programs cannot detect fraudulent traffic that originates from humans, for example, a fraudster getting access to a telecommunications operator's network and using it for calls. This traffic looks like regular and is detected as fraud only when companies start to bill each other. Therefore, in many cases, fraudulent traffic cannot be detected by the receiving party immediately. Moreover, such programs cannot identify fraudulent traffic with absolute accuracy, so, at the moment, the fraud detection process is not fully automatic and requires the participation of humans. Another side of the problem is that not all companies in the market use such softwares in their day-to-day activities.

Another reason for the liability of the traffic originating company is that in many cases, fraudsters act together with the company that sends that traffic, for example, an employee of the company giving access to a fraudster in return for money.[67] The responsibility of the company gives it an additional incentive to conduct internal audits and maintain a proper level of internal security.

This approach is encouraged by the majority of market participants. GLF's code of conduct, which was signed by the biggest carriers including A1 Telekom Austria, Deutsche Telekom, Etisalat, Orange, and others,[68] states that "the originating carrier will remain responsible for the fraudulent traffic and financially liable in case the payment flows cannot be stopped by the downstream carrier(s)."[69]

It must be noted that despite the wide acceptance of the principle of the originating company's liability for fraudulent traffic, some companies still refuse to compensate for the damages, arguing that there was no fault on their side and that the damage resulted from the actions of third parties.[70]

The position of a particular company regarding fraud is not always clear before it happens. For this reason, the clear statement that each company is responsible for the economic losses resulting from fraudulent traffic originated on its own network is an important provision in

[67] LANCK Research Project.
[68] 'Growing Momentum Behind the GLF's Code of Conduct', (*I3FORUM*, 14 June 2018. <http://i3forum.org/blog/2018/06/14/growing-momentum-behind-the-glf-code-of-conduct/>accessed 2 April 2021
[69] Global Leaders' Forum, 'Code of Conduct for International Carriers to take leadership in the prevention of fraudulent traffic' (2018) <http://i3forum.org/blog/2018/05/30/code-of-conduct-to-combat-fraud/> accessed 27 March 2021
[70] LANCK Research Project.

the contract. In this case, the company cannot refuse to pay for fraudulent traffic by claiming that the expenses were a result of a crime.[71]

Establishing the liability for network security in a contract would give an additional responsibility to telecom carriers, as they would make contractual commitments to protect the security of their networks. It would also entail additional expenses, the amount of which depends on the size of the network. For MNOs that usually exercise security control over their networks, the establishment of this principle in the contract would lead to higher level of the said control. For wholesale carriers, it could ensure the relevant protection of their networks. Thus, the total security control in the carrier chain would improve and the number of fraudulent crimes involving hacking of network could decrease.

It is recommended to establish in a contract that each party undertakes to protect the security of its network and shall remain liable for all expenses arising from fraudulent traffic that originates on its respective network.

b) Steps to Follow When Fraudulent Traffic is Detected

Time is a very important factor when the matter concerns a digital crime such as telecom fraud. Prompt actions in fraud detection and the blocking of fraudulent traffic can reduce or even prevent the negative consequences of the crime. Hence, it would be useful to provide in a contract a detailed guidance on what actions must be taken when the fraud is detected and when. Moreover, timely notification to other carriers in the chain and the blocking of the suspected traffic could make the subsequent dispute process easier and faster.

[71] Except for the direct ruling of the national regulatory authority, Par. 13 of the Irish Regulation 23(2) Process-An Operator's Information Note (available at: https://www.comreg.ie/?dlm_download=regulation-232-process-information-note-for-operators) states that Commission for Communications Regulation (ComReg) in case of telecoms fraud incident can issue an interim order requiring the affected operator(s) to withhold the service revenues for the relevant calls for a period of four months. If, after the investigation, ComReg decides that fraud has occurred, the interim requirement may be made permanent. Basically, this rule means that Irish operators shall not pay for fraudulent traffic.

First of all, the contract shall oblige both parties to monitor and analyze traffic patterns to identify and block any fraudulent traffic as soon as possible. If only one party does it, the likelihood of fraud detection decreases. It seems to be a natural obligation of the wholesale carrier; however, it is recommended to expressly include this provision in the contract to avoid a dispute over the originating carrier's liability.

Secondly, the parties to a contract should stipulate a detailed list of concrete actions to be carried out when fraud is detected by both of them. Considering the time factor, it is also important to highlight that these actions shall be taken as soon as possible. As the first step, a party must promptly communicate with the other party if it knows of or reasonably suspects any fraudulent traffic.

The prompt sharing of data is an important aspect of fraud management. Information about the fraudulent portion of traffic should be communicated to the carriers in the chain as soon as possible. The close collaboration of carriers can be effective in stopping fraudulent traffic and/or withholding payment to the fraudster, thereby financially impacting him.

Following such a notification, several actions such as the following shall be taken:

1. The originating party shall immediately stop the flow of fraudulent traffic to the other carrier’s network.
2. The originating party and the carrier shall immediately exchange information to determine the source of the fraudulent traffic immediately after the incident.
3. The carrier has to undertake all necessary actions to prevent the money flow to downstream carriers.

If all these actions are taken promptly, fraudulent traffic could be stopped and the total harm could be reduced. When fraudulent traffic is stopped promptly, on the one side, it prevents the termination of this traffic by the final company in the chain, which in many cases is a participant in the fraud. This action has the same aim as the third point in the list. Usually, the terminating party shall get payment from the originating party. However, when the terminating party does not receive either the fraudulent traffic or payment for it, the fraudster's plan is disrupted. On the other side, promptly stopping the traffic also reduces the number of companies in the chain participating in the transfer, thereby making dispute resolution faster.

c) Established Dispute Resolution Procedures

There are several grounds for raising a dispute in the ITT market. It can be over the applied rates (rate discrepancy), the actual volume of the traffic, etc. Fraud disputes have some specific features that should be reflected in the contract.

For most types of these disputes, companies usually establish a specific floor for initiating a dispute. In other words, if the disputed amount is less than the established amount[72] or the per cent of the total amount of the relevant invoice,[73] the other party shall pay the bill. This is done to avoid a great number of disputes over a small sum of money. However, when it comes to a fraud dispute, the disputed amount can be less than the established floor to initiate a dispute, although this amount may be significant for the other party. Moreover, the other party may refuse to participate in the dispute, so the disputing party would not be able to request documents that are necessary to resolve disputes in the whole chain. Therefore, it is recommended to exclude fraud disputes of this disputed amount limitation, if any.

[72] For example, USD 100.
[73] Usually 1% or 2% of the per cent of the total (excluding VAT) of the relevant invoice amount.

Another important aspect is that fraud disputes can be raised based on alleged or proven fraudulent traffic that is sent. The traffic is officially fraudulent when it is confirmed by relevant authorities like the police. This means that the dispute can be resolved only after obtaining the relevant confirmation document. In this case, the time factor is relevant. Obtaining such official confirmation can take several weeks. In these circumstances, prompt resolution of disputes would not be possible. It is important to establish in the contract an opportunity to initiate a dispute over both alleged and proven fraudulent traffic. This way, the dispute can be started before receiving the confirmation document, which will be provided later. Under this scheme, the other party will consider the case earlier and take appropriate action from its side before the official document is issued (if it has not done so before).

When a dispute arises, it is always required to provide certain confirmation documents. Therefore, the involved parties may include in the contract a list of documents to be provided when raising a fraud dispute. The main document for fraud dispute resolution issued by the relevant authority confirms that a particular traffic was fraudulent. In most cases, such a document is a police report.[74] However, producing a police report is not the only option, for example, in some countries, such documents can be issued by a national regulator. Sometimes, such documents can be issued by international organizations such as INTERPOL.[75] For this reason, it is better to use broader wording like the following: "The originating party shall provide police or other law enforcement authority report with confirmation of its acceptance by authorized officials."

This report shall contain facts indicating that the incident described in the document relates to the dispute, accompanied by the relevant call detail records. Considering that there is no

[74] LANCK Research Project.
[75] International Criminal Police Organization.

comprehensive common form for such reports, there are no universal standards for their content. In some cases, such reports do not contain any information that indicates a connection between the traffic in question and the crime reported in the document. To avoid this situation, it is important to establish in the contract an obligation of the company to include all the required data when filing its report to the relevant authority.

Considering that the time factor is significant, it is also recommended to state in the contract a time limit for the provision of the documents. Since billing periods can be significant in issues of fraud, it would be recommended to provide for a period of 30 calendar days after raising of the dispute. This period is a default in SMS traffic transit contracts and is popular for VOIP contracts as well.[76]

Finally, it must be noted that the successful resolution of fraud disputes depends on the third parties. The involved companies cannot resolve the issue without the relevant authorities (for the issuance of the confirmation documents) and other participants in the carriers' chain. When a dispute arises, a corresponding dispute with the downstream carrier is initiated. The success of the initial dispute depends on the success of the correspondent dispute. The result of the successful resolution of a fraud dispute is the obtaining of a credit note from the company's service provider. Failing to get this document from one carrier in the chain means that all other fraud disputes raised between the participants in the chain will not be resolved. Therefore, it may be useful to establish a connection between the disputes between the parties to a contract and the correspondent dispute that a party will raise with its counterparty that is next in the chain. For example, the parties can establish in a contract that the service providers will endeavor to obtain a credit note from its suppliers. If the credit note cannot be obtained, the originating party shall pay for the fraudulent traffic. Thus, the service provider

[76] LANCK Research Project.

is not obliged to provide the originating party with the credit note if the service provider did not get it from its suppliers.

As previously mentioned in this chapter, it seems clear that a contract can be effective in resolving fraud-related disputes. The parties are free to institute a special set of rules on how to deal with fraud disputes, including procedural issues. The binding force of the contract makes these rules obligatory and enforceable. Furthermore, due to the chain structure of the market, many carriers would like to include corresponding provisions in their contracts with other companies.

At the moment, there is no generally accepted set of rules on how to deal with fraud issues in SMS and VoIP agreements. The level of regulation of these issues depends on the type of the agreement and the kind of company that prepared it. Mobile networks operators tend to draft more detailed contracts that in some cases mention clear fraud-related provisions, including procedural matters. It must be noted, however, that the chain structure of the ITT market requires a uniformity concening these provisions. Setting up a commonly accepted set of rules for fraud dispute resolution would be a step toward tackling the problem.

This paper suggests several recommendations about provisions that should be included in contracts. These recommendations are in line with the principles developed by i3forum, whose participants are the biggest MNOs and wholesale carriers. Establishing a liability of the companies for failure to protect their networks, guidance on actions when the fraudulent traffic is detected, and detailed dispute resolution procedure would contribute to the creation of a common business practice for tackling issues of fraud in the market.

Conclusion

This thesis sought, first, to explore the reasons why fraud is a huge problem for the telecommunications industry, which affects all layers of the market. After a critical examination of the industry's legal response, the thesis addressed the principal question of which legal instrument would be the most effective to tackle the problems arising from fraud disputes among telecom carriers. To answer this question, the research covered the main features of the ITT market, focusing on the reasons for its vulnerability to telecom fraud in conjunction with the empirical data obtained during the LANCK Research Project.

One of the main features of the ITT market is the interconnection and interdependence of telecom carriers. The transfer of traffic from one operator to another can require the participation of several carriers that forms a chain of interconnected companies. Each company in the chain receives and sends traffic to the downstream carrier. This traffic flow is followed by money transfer from one carrier to another. Another important feature of the ITT market is the lack of legal regulations in most of the countries as the service of international transit of telecommunication traffic is usually not subject to national regulation. In the absence of regualtion by public law, carriers use business practices and interconnection agreements as the main sources of regulation.

However, these features are also the reasons for the market vulnerability to telecom fraud. Telecom fraud is attractive for criminals as it is a less risky way to get money, and it has become an industry in itself. The international nature of the crime and technically complexity of the issue make fraudsters largely inaccessible to law enforcement authorities.

Unable to prevent such crimes, telecom carriers have to use alternative instruments to address its consequences. The analysis showed that instruments such as codes of conduct, rules and

principles of the industry, and business practices are not very useful. Considering the main features of the ITT market, interconnection agreements would be the most efficient tool to tackle fraud-related disputes.

The analysis of the empirical data obtained from the LANCK Research Project has demonstrated that contracts are not widely used to address the problem of fraud disputes. As a rule, MNOs include fraud-related provisions in their contracts more often than wholesale carriers. However, the rules and principles provided in the operators' agreements still lack a uniform approach toward solving the problem.

To tackle this problem, the thesis proposes the stipulation of some rules and principles in the contracts of all participants in the chain. First of all, it is important to maintain that parties are liable for the integrity and security of their networks. Secondly, it is recommended to discuss the steps that shall be taken by both parties when fraudulent traffic is detected. Third, it would be useful to lay down a detailed dispute resolution procedure in contracts, including a list of the required documents and time frames. The inclusion of these provisions in interconnection agreements would make the procedure of fraud dispute resolution faster and simpler.Additionally, it can affect companies that do not have these provisions in their contracts by shaping the common business practice of the industry. The findings and recommendations set out in this thesis can thus be used by telecom carriers for drafting their contracts. Additionally, this thesis can provide a basis for further research on the issue of telecom fraud in the wholesale telecom market.

Glossary

Subscriber	the ultimate user of a telecommunications service
Telecom carriers	all types of companies providing telecommunication services as their main business activity to subscribers, enterprises and telecom service providers.
Telecom network	a system of physical communication channels and switching equipment to transmit telecom traffic
Telecom traffic	the amount of data moving across networks of telecoms carriers
Voice over Internet Protocol (VoIP)	technology for making voice calls using an Internet connection instead of analogue phone lines
Wholesale carrier	an entity that operates a telecom network and provides telecoms services to other telecom carriers
Wholesale telecom market	a type of telecommunications business where telecom carriers provide services to each other

Bibliography

Bourreau M, Hombert J, Pouyet J and Schutz N, *Wholesale Markets in Telecommunications-CEPREMAP*, (June 2007)

Global Leaders' Forum and Delta Partners, *Taking Action Against Fraud Demonstrating the International Wholesale Industry's Leadership Against Telecoms Fraud* (October 2018) < https://www.deltapartnersgroup.com/sites/default/files/GLF%20-%20Taking%20Action%20Against%20Fraud%20-%20October2018_0.pdf>accessed 17 March 2021

Global Leaders' Forum, *Code of Conduct for International Carriers to Take Leadership in the Prevention of Fraudulent Traffic* (2018) <http://i3forum.org/blog/2018/05/30/code-of-conduct-to-combat-fraud/> accessed 27 March 2021

Greatrex M, 'The Pursuit of Certainty: A New Approach to Best Endeavours Clauses.' (2019) 25 AULR

GSM Association, *Fraud Manual*, version 16.0 (08 August 2018)

i3forum, 'Growing Momentum Behind the GLF's Code of Conduct', (14 June 2018) <http://i3forum.org/blog/2018/06/14/growing-momentum-behind-the-glf-code-of-conduct/>accessed 2 April 2021

International Interconnection Forum for services over IP, 'Fraud Classification and Recommendations on Dispute Handling within the Wholesale Telecom Industry' (*I3FORUM*, May 2014). <http://i3forum.org/blog/2014/05/01/fraud-classification-and-recommendations-on-dispute-handling-within-the-wholesale-telecom-industry-release-3-0-may-2014/> accessed 12 January 2021

Johansson E, 'Wholesale telecom Needs to Take Advantage of Digitalization Opportunities' *Verdict* (25 June 2020). <https://www.verdict.co.uk/telecom-wholesale> accessed 15 January 2021

Kozuka S, 'The Economic Implications of Uniformity in Law. Uniform Law Review', (2007) 12(4) RDU

Lessig L, *Code and Other Laws of Cyberspace* (Basic Books 1999)

OCCPR Report of March 2019. <https://www.occrp.org/en/daily/9436-report-us-32-7-billion-lost-in-telecom-fraud-annually> accessed 23 January 2021

Trend Micro Research Europol's European Cybercrime Centre (EC3), Cyber-Telecom Crime Report 2019. <file:///D:/cyber-telecom_crime_report_2019_public.pdf> accessed 20 January 2021

Walden I(ed), *Telecommunications Law and Regulation* (Oxford University Press, 2018)

Walden I, *Computer Crimes and Digital Investigations* (2nd edn, Oxford University Press, 2016)

Wall DS, 'Policing Cybercrimes: Situating the Public Police in Networks of Security Within Cyberspace', [2007] 8(2) PPR 183–205 [DOI: 10.1080/15614260701377729].