CEPT ECC
Electronic Communications Committee

ECC Report 275

The role of E.164 numbers in international fraud and or misuse of electronic communications services

approved 30 May 2018

0 EXECUTIVE SUMMARY

Fraud and misuse has always been an issue in the telecommunications industry and CEPT countries are increasingly faced with fraud and misuse where E.164 numbers play a role. As technology has developed, particularly on the Internet, end-users have much more access to, and control over, communications networks. This has been a welcome development for the vast majority of end-users in terms of choice and access to applications and services but the negative impact is that it has also made fraud and misuse much easier to perpetrate. Fraud and misuse is now a global problem where jurisdiction is increasingly becoming a major challenge.

For example, fraudsters deliberately take advantage of the inherent trust that end-users have in Calling Line Identification (CLI) (e.g. by spoofing valid numbers as CLI) in order to perpetrate fraud during telephone calls (e.g. to elicit bank account details, credit card details or other types of personal information). In many cases, the techniques are automated and originate in developing countries and/or in unstable jurisdictions where fraudsters know they are relatively safe from detection and prosecution.

International Revenue Share Fraud (IRSF), a form of fraud whereby the perpetrator artificially inflates traffic by generating calls to certain portions of national number ranges in different countries, is the top ranking type of telecom fraud worldwide, according to a 2017 report [13] by the Communications Fraud Control Association (CFCA). The worldwide losses caused by IRSF – in 2017 estimated to be US$6.1 billion – is almost 50% more than that caused by the second ranking type of fraud (interconnect bypass) which is estimated to be US$4.27 billion. According to the CFCA report, the top five countries where fraudulent calls (in general) terminate are Cuba, Latvia, Lithuania, UK and Tunisia. The top five countries where fraudulent calls originate are the United States, Spain, UK, Russia and Palestine. The CFCA report also notes that global telecom fraud decreased 23.3% (from over US$38 billion to US$29.2 billion) since the last global fraud loss survey (2015). However the ECC, in its discussions with some industry players, notes that the numbers of complaints from operators about fraud are increasing. Therefore telecom fraud is still a problem that must be addressed.

Chapter 3 of this report examines the motive, method and opportunity for committing fraud. An inventory of known fraud and misuse methods are grouped into two broad categories. The first category is based on misusing the payment and settlement arrangements between operators which are based on roaming and interconnection agreements. The second category is those types of fraud and misuse that take place during a communications session with an end-user. A combination of techniques may be used in many cases and this report focuses on those techniques where E.164 numbers play a role.

Chapter 4 examines the administrative tools that have been developed to tackle fraud and misuse of E.164 numbers. The International Telecommunication Union (ITU), Electronic Communications Committee (ECC), Body of European Regulators for Electronic Communications (BEREC) and the European Union (EU) have all developed policies, regulations and guidelines on different aspects of fraud and misuse.

Chapter 5 focuses on measures implemented in European Conference of Postal and Telecommunications Administrations (CEPT) countries to tackle fraud and misuse of E.164 numbers and CLI spoofing. This information is based on a recent survey of CEPT countries covering rules on CLI, CLI spoofing and measures taken at the national level to tackle fraud and misuse.

Chapter 6 provides information on initiatives to tackle fraud in the US. Federal Communications Commission (FCC) and measures to tackle robocalls and telemarketing calls are discussed. This chapter also covers initiatives by the Internet Engineering Task Force (IETF) to tackle fraud on IP-based networks and tools that are available to network providers and end-users to block calls.

Chapter 7 examines technical measures that can be implemented to detect and prevent the different fraud and misuse techniques.

Chapter 8 studies the roles and responsibility of the different operators in the value chain and how they can provide a “duty of care” to their customers. This goes beyond just acting according to the law. Operators

should, if they have knowledge that misuse or fraud is directly or indirectly taking place using their networks, follow ethical standards and take whatever action is necessary in a proportionate way to protect end-users.

Chapter 9 explores the competence of different authorities to tackle fraud and misuse. In most CEPT countries, it is the law enforcement authorities that have competence to tackle fraud and National Regulatory Authorities (NRAs) or the competent telecommunications authorities may only be involved in an informal way in assisting with the investigation of fraud schemes as described in this report. NRAs or the competent telecommunications authorities normally have a formal role to play regarding the misuse of E.164 numbers.

Chapter 10 provides information on international cooperation which is necessary to tackle cross-border fraud where jurisdiction is a major difficulty. International cooperation is also vital to minimise the misuse of E.164 numbers.

Chapter 11 makes recommendations for best practices.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Abbreviation	Explanation
BEREC	Body of European Regulators for Electronic Communications
CEPT	European Conference of Postal and Telecommunications Administrations
CFCA	Communications Fraud Control Association
CLI	Calling Line Identification
ECC	Electronic Communications Committee
ECS	Electronic Communication Services
EECC	European Electronic Communications Code
EU	European Union
FCC	Federal Communications Commission
FMC	Fixed Mobile Convergence
GSMA	Global System for Mobile Communications Association or GSM Association
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IRSF	International Revenue Share Fraud
ISUP	Integrated Services Digital Network (ISDN) User Part
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
IVR	Interactive Voice Response
M2M	Machine-to-Machine
MSISDN	Mobile Subscriber ISDN Number
NRA	National Regulatory Authority
OEM	Original Equipment Manufacturer
OTT	Over-The-Top
PBX	Private Branch Exchange
SHAKEN	Signature-based Handling of Asserted information using tokens
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SS7	Signalling System No. 7
STIR	Secure Telephony Identity Revisited

Abbreviation	Explanation
USD	Universal Service Directive
VoIP	Voice over Internet Protocol
WAP	Wireless Application Protocol
WTSA	World Telecommunication Standardization Assembly

1 INTRODUCTION

CEPT countries are increasingly faced with fraud and misuse where E.164 numbers play a role. For example, fraudsters deliberately take advantage of the inherent trust that end-users have in CLI (e.g. by spoofing valid numbers as CLI) in order to perpetrate fraud during telephone calls (e.g. to elicit bank account, credit card details or other types of personal information). In many cases, the techniques are automated and originate in developing countries and/or in unstable jurisdictions where fraudsters know they are relatively safe from detection and prosecution.

Fraud and misuse have always been an issue in the telecommunications industry. As technology has developed, particularly on the Internet, end-users have much more access to, and control over, communications networks. This has been a welcome development for the vast majority of end-users in terms of choice and access to applications and services but the negative impact is that it has also made fraud and misuse much easier to perpetrate and it is now a global problem where jurisdiction becomes a major challenge. International cooperation and solutions are necessary to address this phenomenon.

This report makes an inventory of known fraud and misuse techniques and is followed by a description of the ecosystems within which fraud and misuse are enabled. A summary is then provided of the existing rules and regulations (national and international) to maintain trust in the telephone numbering system.

Some measures are then proposed to minimise fraud and misuse and to mitigate the negative effects for users taking into account that some fraudsters deliberately do not behave according to the rules and procedures. These measures can be based, amongst other things, on practices in the Internet ecosystem.

One important aspect studied is the responsibility of the different entities in the value chain and what can be reasonably expected from these entities in terms of providing a "duty of care" to protect end-users.

For the sake of clarity fraud between operators, harassment, unwanted marketing calls or fraud and misuse where E.164 numbers do not play a role are considered outside of the scope of this report. The main focus of the report is on fraud and misuse perpetrated using electronic communications voice services.

2 DEFINITIONS

Term	Definition
Calling Line Identification Presentation	According to ITU-T Recommendation E.157, Calling Line Identification (CLI) Presentation is a supplementary service offered to the called party which provides the calling party's number, with additional address information (e.g. calling party sub-address) if available, to the called party.
Fraud	Wrongful or criminal deception intended to result in financial or personal gain.
Misuse of a E.164 number	Misuse of an international E.164 numbering resource occurs where the use of that numbering resource does not conform to the relevant national numbering plan and/or relevant ITU-T recommendation(s), assignment criteria for which it was assigned or when an unassigned numbering resource is used in the provision of a telecommunication service.
Calling/Caller ID spoofing	A technique that enables the calling party, originating network and/or transit network to manipulate the information displayed in the CLI field with the intention of deceiving the called party into thinking that the call originated from another person, entity or location.
Refiling/re-origination	Refiling or re-origination is the name given to the practice of substituting the CLI for the call at some point in the call session. Refiling or re-origination is made possible by exploiting the functionality of the signalling system which allows for a great deal of call information to be transmitted. In principle, a terminating operator can inspect the CLI to see where the call has originated and change accordingly. In practice, switches have the capability to remove or change the CLI, thus disguising the origin of the call.

3 TELECOMS FRAUD AND MISUSE - MOTIVE, METHOD AND OPPORTUNITY

In dealing with any crime, one must be able to identify the motive (e.g. financial gain) and the method (tools and techniques). Where there is motive and method, then opportunities for fraud and misuse will exist. In order to minimise telecom fraud and misuse involving E.164 numbers, and taking into account that regulators have little impact on the motive, the only solution is to make the methods impossible thereby eliminating the opportunity.

In this section different techniques to perpetrate fraud and misuse are identified and described. E.164 numbers play a role in many of these techniques to varying degrees and, in practice these different techniques are often combined to commit fraud and misuse. **This Report is focused on addressing instances of fraud and misuse where E.164 numbers play a role and where the inherent trust that end-users have in E.164 numbers is exploited.**

3.1 FRAUD AND MISUSE TECHNIQUES

3.1.1 CLI Spoofing

"CLI Spoofing" is a technique that enables the calling party, originating network and/or transit network to manipulate the information displayed in the CLI field with the intention of deceiving the called party into thinking that the call originated from another person, entity or location. Fraudsters use CLI spoofing to take advantage of the inherent trust that end-users have in the integrity of CLI information. Normally, the CLI presented is a national geographic or mobile E.164 number with a format that the called party would be familiar with. With CLI spoofing the number displayed could be an unassigned number or one which is already assigned to another end-user. End-users whose numbers have been used in CLI spoofing scams often need to change their number as they may receive many calls from victims of the spoofing scam. The use of Voice over Internet Protocol (VoIP) client software provides the control to change CLI information and this control can be misused by fraudsters. ECC Report 248 [4] contains further information on flexible CLI usage, which has advantages for end-users when it is not used with malicious intent.

3.1.2 Refiling/re-origination of traffic

Refiling/re-origination is a technique which is based on manipulation of the “A number” by the fraudster. Refiling/re-origination creates problems not only for the operator which terminates the call, but also for the end-user because if the end-user tries to dial this number, it will not be possible to reach the calling party.

This is a technique that has become increasingly popular in last two years. The reason for this is the difference in call termination tariffs between operators of European Economic Area (EEA) member states and operators outside the EEA. The “A number” of the country outside the EEA is replaced with a number from an EEA country. The number which is displayed could be an unassigned number or one which is already assigned to another end-user. Usually refiling/re-origination is done by a transit operator but it is not excluded that it could be done by the operator who originated the call.

The impact of refiling/re-origination is that it negatively affects the revenues of operators from within the EEA but also negatively impacts the end user e.g. CLI spoofing or inability to initiate a call back. Finding the fraudster is very difficult. One approach is to follow the chain of involved transit operators, starting with the operator who delivered the call to the terminating network. Refiling/re-origination is technically possible using Signalling System No. 7 (SS7) and SIP signalling.

3.1.3 Wangiri (or ping calls)

The fraudster originates, usually via an automated technique, high volumes of very short calls to a whole range of numbers. These calls are dropped after one or two rings so that they appear as missed calls on the end-user's display. The fraudster anticipates that the called end-users will see the missed call and call back. The CLI displayed does not identify the actual calling line as the CLI is spoofed. The CLI does not always display a geographic or mobile number. Other numbers such as premium rate numbers or high tariff destination numbers are also displayed. The fraudsters anticipate that many end-users will call back without noticing that the called number is a high tariff number until they receive their monthly bill. In many cases callers are connected to Interactive Voice Response (IVR) systems which play recorded messages to keep them on the line as long as possible.

As the initial call is very short it is rarely answered. Therefore, no call charges are applied so this technique is very cheap for fraudsters to implement and can be easily automated. Another similar technique involves the presentation of a valid premium rate or high tariff number to which the fraudster has been granted a right of use. However, the opportunity for this type of fraud is limited as the presentation of premium rate numbers as CLI is prohibited in most countries.

In other cases, a regular number (usually a national mobile number since the likelihood of the call being answered by the called party is higher) is spoofed as CLI by the fraudster. If the called party answers or calls back they hear a recorded message prompting them to call a high tariff or premium rate number. They will then receive an offer (e.g. to cancel a debt, to claim a gift, or to avail of a job offer).

Call back rates for wangiri can potentially be surprisingly high – an ‘effective’ attack can be up to between 10 to 15% of a call back rate. Even assuming a lower call back rate of for example 1% the overall impact on end-users can be significant.

Variants of this type of fraud and misuse exist where the initial short call is replaced by an SMS or social media message where the called party is alerted or incentivised to call a number contained in the message. These numbers can be displayed as hyperlinks on smartphone displays and this increases the likelihood of a return call being made. Nevertheless these variants appear to be less effective than if the first leg is a voice call.

3.1.4 Hacking of accounts/PBX

The fraudster hacks a subscriber's telephone account or a corporate Private Branch Exchange (PBX). Artificial traffic (i.e. simulated traffic) can then be generated to premium rate numbers or other high tariff numbers. Even legitimate traffic can be rerouted or forwarded in this way. PBX hacking is often used in conjunction with call hijacking or short stopping (discussed in Section 3.1.6). In these cases the fraudsters benefit from the termination of the simulated traffic to high tariff numbers (where revenue share agreements are in place) while the victims whose accounts or PBXs were hacked are billed for the call origination charges.

3.1.5 Traffic collectors and roaming fraud

Fraudsters use Subscriber Identity Module (SIM) boxes or other devices to generate artificial or inflated traffic to specific high tariff or premium rate numbers known as "traffic collectors". Originating calls are concentrated around certain cell areas and usually do not make any calls to any other numbers except the "traffic collectors".

This type of fraud is often based on using stolen SIM cards from travellers roaming in other countries. The fraudsters take advantage of using these SIMs on a visited network to generate a large volume of calls to high tariff numbers before the home network is able to block the SIM based on a report from the customer or the visited network operator[1].

These practices are easily detected by telecom operators as network traffic analysers can detect sharp increases of originating traffic in certain cell areas and of increases in traffic destined for termination to certain numbers.

[1] The ECC understands that there is a delay before information is exchanged between the visited network and the home network on abnormal traffic patterns

3.1.6 Call hijacking / short stopping

Normally a call flows from the originating operator, via one or more transit operators to the terminating operator to which the called end-user is attached. Sometimes it is possible that a dishonest or unscrupulous operator will terminate the call on their networks before it reaches the destination. This type of fraud is often referred to as call hijacking or short stopping. Call hijacking and short stopping are very similar by routing technology but may be different by the type of destination numbering used. There are two main variations of this:

- In the first variation, a proportion of legitimate call traffic is intercepted by a transit operator and terminated on the transit operator’s network, usually to a recorded announcement. The transit operator charges the full wholesale transit charge and therefore has a very high margin on all calls routed to the recorded announcement. The transit operator may further benefit if the original caller attempts to make a call for a second time after having received the recorded announcement the first time. With this type of fraud, it is very often the case that only a proportion of the traffic is rerouted to unassigned numbers which may be connected to an IVR system. This is done to prevent a large number of end-user complaints so that the originating operator has no basis to initiate an investigation. As the majority of traffic is terminated correctly, this type of fraud can be difficult to detect without a detailed analysis of call traffic. This variation is often used in conjunction with PBX-hacking (discussed in Section 3.1.4) where genuine or artificially generated traffic is routed to the hacked PBX and sent to different national or international destination numbers. These numbers could be premium rate numbers, high tariff destination numbers, numbers assigned to another service provider or unassigned numbers used for fraudulent purposes.
- In the second variation, content providers, mainly premium rate content providers, advertise their services on media in multiple countries enticing viewers to call a high tariff destination number. The transit operator involved with the content provider can then intercept the traffic and short stop it in a country closer to the originating caller. The transit operator benefits from the higher margin on short stopped calls and the content provider benefits from being able to circumvent premium rate services regulation in the country where the services are advertised.

3.1.7 Subscription fraud

Fraudsters subscribe to telecom services with no intention of ever paying the invoice. Typically they use false identities, fake companies and stolen credit card details to subscribe to a service and then disappear after some months. This type of fraud is often combined with "traffic collectors" (discussed in Section 3.1.5).

Another form of subscription fraud is where end-users unwittingly subscribe to services when they click on links in web pages (pop-ups) on the Internet when using mobile data. The subscription charge appears on the end-users telephone bill. The mobile operator uses a procedure called Wireless Application Protocol (WAP) billing for this purpose. WAP billing is a legitimate technology but is abused by fraudsters who develop a type of malware known as "trojans" which covertly subscribe to "services" owned and controlled by fraudsters. When WAP billing is used legitimately end-users are notified, usually by SMS, that they are subscribing to a service and the message provides information on the associated charges and an option to opt-out. However, fraudsters exploit the fact that when tablets, broadband dongles or data-only SIMs without SMS capability are used the end-user never receives this information. End-users need to be vigilant and ensure that they pay careful attention to any additional charges on their telephone bills.

Additionally, there is a privacy issue related with WAP billing. The end-user's mobile number Mobile Subscriber ISDN Number (MSISDN) is received by the fraudster as this information is included in the HTTP header included in a WAP subscription request (e.g. X-UP-CALLING-LINE-ID, X-MSISDN). Mobile operators should explore the possibility of using alternative identifiers in the HTTP header for WAP billing.

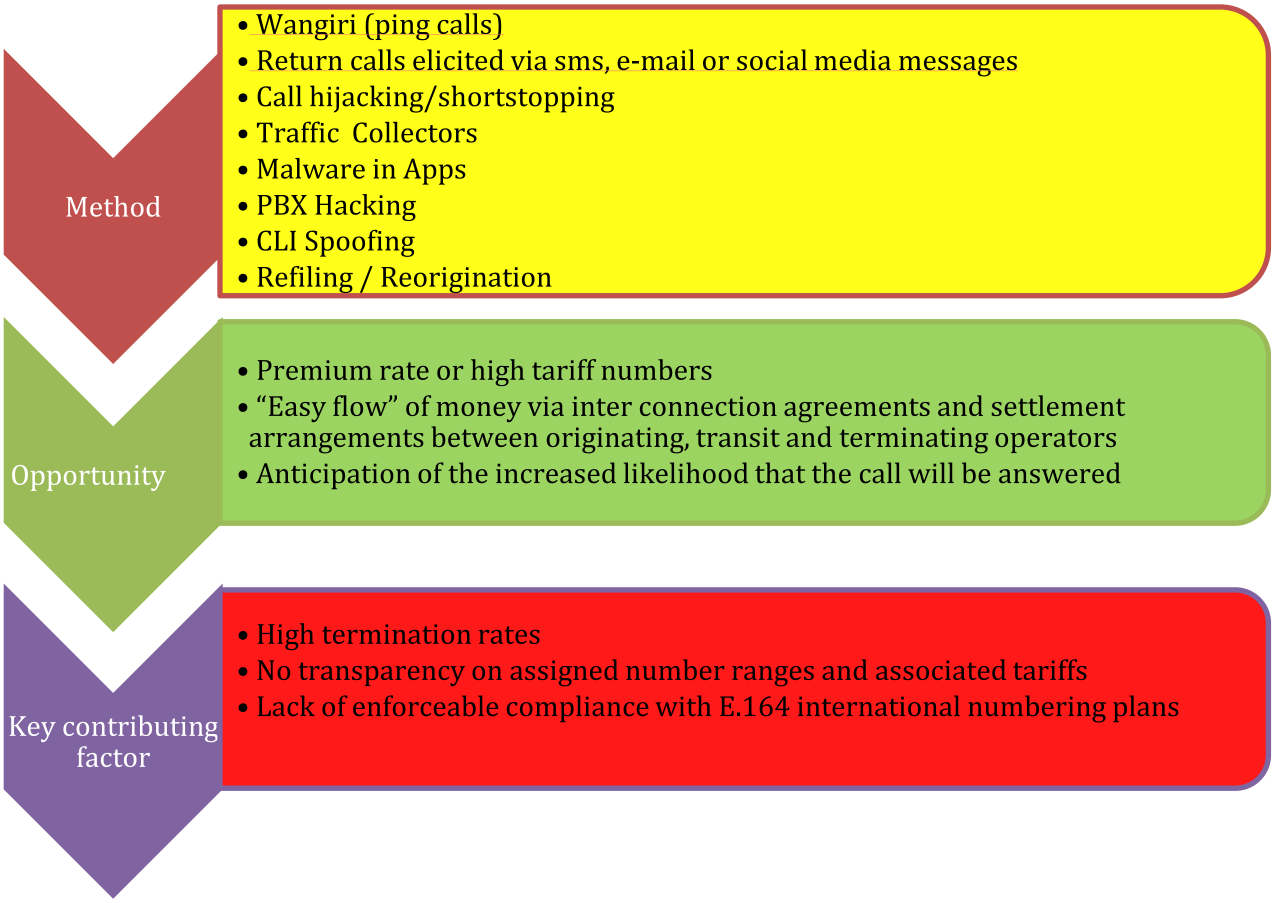
3.1.8 Malware in apps

Some smartphone apps (usually adult content apps) downloaded from unofficial app stores contain malware that can generate calls to high tariff or premium rate numbers while they are being used or even when the smartphone is in idle mode. The end-users will be unaware that the calls have been made until they notice that the credit has expired or receive their bill.

3.2 FRAUD AND MISUSE CATEGORIES

In this section, the different fraud and misuse techniques identified and described in section 3.1 are categorised into two broad categories. The first category is based on misusing the payment and settlement arrangements between operators (i.e. where there is an impact on money flow between operators) which are based on roaming and interconnection agreements. The second category is based on the types of fraud and misuse that take place during a communication session with an end-user (i.e. where there is no impact on money flow between operators). A combination of the techniques described in section 3.1 may be used to perpetrate fraud.

3.2.1 Money flow via originating telecom operators to terminating (or transit) operators



Method

- Wangiri (ping calls)
- Return calls elicited via sms, e-mail or social media messages
- Call hijacking/shortstopping
- Traffic Collectors
- Malware in Apps
- PBX Hacking
- CLI Spoofing
- Refiling / Reorigination

Opportunity

- Premium rate or high tariff numbers
- “Easy flow” of money via inter connection agreements and settlement arrangements between originating, transit and terminating operators
- Anticipation of the increased likelihood that the call will be answered

Key contributing factor

- High termination rates
- No transparency on assigned number ranges and associated tariffs
- Lack of enforceable compliance with E.164 international numbering plans

Figure 1: Fraud and misuse scenarios where money flow takes place via operators

Operators are contractually bound by interconnection agreements at the national and international levels. The terms of these agreements are commercial in nature and are normally agreed bilaterally by contracting parties. It is typical for these agreements to require the originating operator to pay for all calls originating from its network whether it is fraud or not. Fraud perpetrated in an international setting where money flow takes place between operators across international borders is known as International Revenue Share Fraud (IRSF). The impact of IRSF is discussed further in Chapter 7.

3.2.2 Fraud and Misuse that takes place during a communication session with an end-user

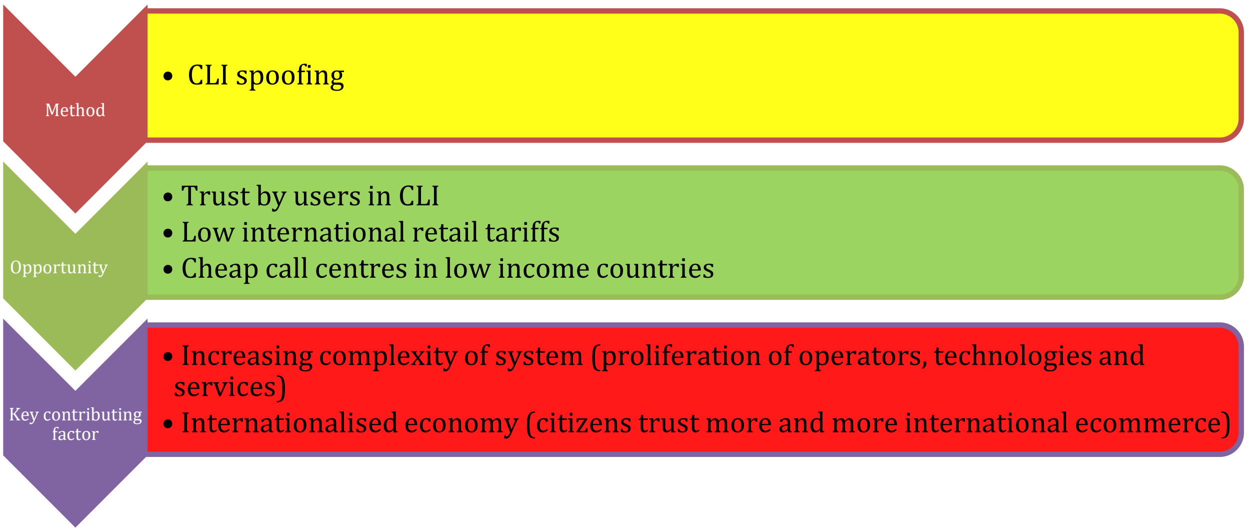

Method
• CLI spoofing
Opportunity
• Trust by users in CLI
• Low international retail tariffs
• Cheap call centres in low income countries
Key contributing factor
• Increasing complexity of system (proliferation of operators, technologies and services)
• Internationalised economy (citizens trust more and more international ecommerce)

Figure 2: Fraud and misuse scenarios that take place during a communications session

End-users receive calls from fraudsters using a CLI which looks familiar and creates trust. A typical example that has been prevalent in Europe in recent years is where the caller claims to be a computer security expert from a global software supplier and that the end-user's PC or laptop has been infected with malware. The fraudster offers to resolve the issue and will ask the end-users to give them remote access to their PC or laptop. They will then use that access to get hold of personal data. In other variants, the fraudster offers a tool which the end-users can download to "fix" the problem which turns out to be malware or the fraudster simply asks the end-users for money (e.g. where the victim provides credit card details) in return for a lifetime of "protection" from the malware they pretend is on their device.

4 INVENTORY OF ADMINISTRATIVE TOOLS TO AVOID FRAUD AND MISUSE OF E.164-NUMBERS

In order to counteract the identified fraud and misuse techniques (wangiri, CLI spoofing, call hijacking etc.), we have to avoid the misuse of E.164 numbers and associated CLI facilities for making calls.

4.1 MISUSE OF CLI

The ECC has already produced some deliverables associated with CLI with the purpose of minimising the misuse of numbers as CLI. These deliverables include:

- ECC Report 133 [2] - "Increasing Trust in Calling Line Identification and Originating Identification";
- ECC REC (11)02 [3] - Calling Line Identification and Originating Identification";
- ECC Report 248 [4] - "Evolution in CLI usage – decoupling of rights of use of numbers from service provision".

ECC Report 248 takes into account developments in technology, such as OTT services, which allow for more flexible use of CLI. The report examines several scenarios of flexible CLI use and draws attention to the possibility of misusing this greater flexibility. The report calls for regulatory intervention including the use of CLI validation techniques.

Also ITU-T has studied this issue and has developed the following recommendation related to the use of CLI in the International telecommunication networks:

- ITU-T Recommendation E.157 [6] - "International calling party number delivery".

ITU-T also specifies most of the signalling systems (e.g. SS7/ISUP) in use, where there are several rules for the modification/manipulation of the content included in the CLI (e.g. deleting/adding country code).

It should also be mentioned that the EC e-privacy directive[2] has defined some rules related to the use of CLI, mainly associated to supplementary services (e.g. Presentation/Restriction of CLI).

4.2 MISUSE OF E.164 NUMBERS

This section provides an overview of identified instruments offered by ITU, EU and ECC to avoid misuse of E.164 numbers.

4.2.1 ITU

World Telecommunication Standardization Assembly (WTSA) Resolution 20, (Hammamet, Tunisia) resolves to instruct *"Study Group 2 of the ITU-T, in liaison with other relevant study groups, to provide to the Director of TSB: ii) information and guidance in cases of reported complaints about misuses of international telecommunication NNAI*[3] resources" *and* "the Director of TSB, in close collaboration with Study Group 2, and any other relevant study groups, to follow up with the administrations involved on the misuse of any international telecommunication NNAI resources and inform the ITU Council accordingly".

Furthermore Resolution 20 resolves to instruct the Director of TSB to "take the appropriate measures and actions where Study Group 2, in liaison with the other relevant study groups, has provided information, advice and guidance in accordance with resolves to instruct 2 and 3 above*" and resolves to instruct "Study Group 2 to continue to study necessary action to ensure that the sovereignty of ITU Member States with*

[2] The EC has published a draft regulation on e-privacy which is currently being discussed

[3] Numbering, naming, addressing and Identification resources

regard to country code NNAI plans is fully maintained, including ENUM as enshrined in Recommendation ITU-T E.164 [7] and other relevant Recommendations and procedures; this shall cover ways and means to address and counter any misuse of any international telecommunication NNAI resources".

The new resolution "Enhancing access to an electronic repository of information on numbering plans published by the ITU Telecommunication Standardization Sector (Hammamet, 2016)" indirectly touches on the fact that creating more transparency in numbering plans could assist in countering misuse of international numbering resources.

With regards to transparency, resolves 3 of WTSA Resolution 61 (Dubai, 2012) invites Member States *"to encourage administrations and national regulators to collaborate and share information on fraudulent activities related to misappropriation and misuse of international numbering resources, and to collaborate to counter and combat such activities"*. It further resolves *"that administrations and operating agencies authorized by Member States take, to the furthest extent practicable, all reasonable measures to provide information necessary to address issues related to number misappropriation and misuse"* and *"that administrations and operating agencies authorized by Member States should take note of and consider, to the furthest extent practicable, the "suggested guidelines for regulators, administrations and operating agencies authorized by Member States for dealing with number misappropriation", in accordance with the attachment to this resolution".*

Regarding countering fraudulent number misappropriation and misuse, in resolves 5 invites Member States *"to encourage administrations and international telecommunication operators to implement ITU-T Recommendations in order to mitigate the adverse effects of fraudulent number misappropriation and misuse, including blocking of calls to certain countries"*. Besides, it resolves further *"to request Study Group 2 to study all aspects and forms of misappropriation and misuse of numbering resources, in particular of international country codes, with a view to amending Recommendation ITU-T E.156 [5] and its supplements and guidelines to support countering and combating these activities"*; *"to request ITU-T Study Group 3, in collaboration with Study Group 2, to develop definitions for inappropriate activities, including inappropriate activities causing loss of revenue, related to misappropriation and misuse of international numbering resources specified in the relevant ITU-T Recommendations, and to continue to study such matters"*; and *"to request Study Group 3 to study the economic effects resulting from misappropriation and misuse of numbering resources, including call blocking"*.

The CEPT submitted a European Common Position (ECP) to WTSA-16 aiming to amend Resolution 61 to further clarify the scope of the technical studies to be undertaken in relation to misappropriation and misuse of international telecommunication numbering resources. Europe believes that potential action by Member States can be further developed – especially as there are new forms of misappropriation and misuses of international telecommunication numbering resources being instigated since Resolution 61 was approved in 2008. As part of the development of further actions, the ECP stated that there is a need to be specific in the actions that can be taken, and, in line with the role of lead study groups, a need to clarify what potential actions should be specified in amending the current ITU-T recommendations. Following the measures specified in the Universal Service Directive of the European Union (USD), amongst the amendments proposed, the selective blocking or the withholding of interconnection payments for particular international numbers, authorised on a case-by-case basis from national regulators, it is considered preferable instead of the blocking of calls to certain country codes. The ECP also proposed guidelines on how to act when complaints regarding number misappropriation are received in the originating country.

Although consensus was not reached to amend Resolution 61, it is clear that there is a concern on the part of European countries to act in a coordinated way to counter fraudulent activities related to misappropriation and misuse of international numbering resources.

It is clear that the ITU will not intervene in any disputes concerning numbering resources assigned to Member States and remains in a pure role of facilitating interactions between the different stakeholders. In that regard, ITU-T SG2 has developed Recommendation E.156 which provides guidelines for ITU-T action on reported misuse of E.164 number resources. ITU-T Recommendation E.156 is currently under review.

4.2.2 EU

Article 28(2) of the USD states that *"Member States shall ensure that the relevant authorities are able to require undertakings providing public communications networks and/or publicly available electronic communications services to block, on a case-by-case basis, access to numbers or services where this is justified by reasons of fraud or misuse and to require that in such cases providers of electronic communications services withhold relevant interconnection or other service revenues".* This provision is currently under review in the European Electronic Communications Code (EECC) but the principles are expected to remain the same.

In 2013, BEREC published guidelines [8] on a cooperation procedure between NRAs in cases of fraud and misuse across country borders. The report highlighted the background to fraud or misuse and its potential impact on end-users through falling foul of instances of fraud or misuse, or for example through a potential lack of confidence in the integrity of numbers. The procedure defined in the BEREC guidelines has been applied very few times.

Annex C of the Authorisation Directive which summarises the conditions which may be attached to the right of use for numbers remains unchanged in the proposed EECC and offers possibilities to attach usage conditions applicable only to the entities to which numbers are assigned in order to combat fraud and misuse. Based on this provision no usage conditions can be attached to operators which intervene in the routing of a call. The EC considers there to be a considerable risk of fraud associated with the extra-territorial use of numbers and proposes in the EECC to limit extra-territorial use to services other than interpersonal communications services (e.g. Machine-to-Machine (M2M)/ Internet of Things (IoT)).

4.2.3 ECC

On October 10th 2007 the ECC adopted Recommendation ECC/REC/(07)02 "Consumer Protection against Abuse of High Tariff Services" [17] based on ECC Report 86 "Consumer Abuses and Fraud Issues Related to High Tariff Services" [18] which was adopted on September 29th 2006. These instruments focus on measures to minimise fraud and misuse of national premium rate numbers. Many of the proposed rules are implemented at the national level.

The main measures recommended in ECC/REC/(07)02 are as follows:

- that the basic telephone service is decoupled from the provision of high tariff services so that the basic telephone service may not be suspended in the case of non-payment of sums relating to high tariff services;
- that high tariff services should only be allowed in appropriate numbering ranges that are allocated for these services, and that are preferably defined in a national numbering plan to facilitate tariff transparency and call barring;
- that the NRA should have the power to impose or modify conditions on the use of a number to address problems when they arise;
- that consumers are well informed by the premium rate service provider about the tariff and content of high tariff services by clear and unambiguous announcements where appropriate and clear announcements of numbers and tariffs at the beginning of calls;
- that, where technically possible, the tariff rate, the duration of a call, or the total cost of a call, or the total amount of the telephone bill should be subject to limitations according to consumer preferences;
- that consumers are enabled to block number ranges in order to prevent the usage of high tariff services in appropriate cases;
- that there is a rapid response mechanism to suspend payments or to block access to numbers while problems and abuses are investigated;
- that appropriate means are established to provide refunds and compensation for consumers who suffer from abuses and unauthorised calls, if necessary after a prior decision of the competent public authorities.

Also Recommendation ECC/REC/(05)09 "Customer Protection in Case of Misuse or Unauthorized Use of International E.164 Numbering Resources" [19] which was adopted on March 14th 2006, contains measures to stop Internet dial up scams based on international numbers.

The main measures recommended in ECC/REC/(05)09 are as follows:

- that NRAs, in co-operation with relevant parties, investigate measures to identify international E.164 numbering resources that are being misused or that are used in an unauthorized manner;
- that NRAs exchange information on international E.164 numbering resources that on a national level are suspected to be misused or used in an unauthorized manner or that have been recognized to be misused or to be used in an unauthorized manner;
- that NRAs, in co-operation with market parties, establish means to protect customers from unintentionally establishing a connection to numbers that are being misused or that are used in an unauthorized manner;
- if the measures mentioned above are not effective enough the CEPT countries reserve the right to suspend the international traffic to the misused international E.164 numbering resources after an official communication by the ECC.

Furthermore, Annex 1 of ECC/REC/(05)09 outlines some principles for an "Early Alert System". This is described as a system of information exchange about suspected or established misuse or unauthorised use of international E.164 numbering resources. Annex 2 contains a list of possible measures for customer protection in case of misuse or unauthorised use of international E.164 numbering resources, including that operators may suspend direct dial access of all calls to the number in question or to the range containing the number, and that NRAs may allow subscribers to refuse to pay the part of the invoice corresponding to the destinations in question on the basis of a code of conduct between different parties.

5 MEASURES IMPLEMENTED IN CEPT COUNTRIES TO TACKLE FRAUD AND MISUSE OF E.164 NUMBERS AND CLI SPOOFING

Telecoms fraud and misuse has increasingly become an issue as technology has evolved. The deployment of IP-based networks, provision of VoIP services and uptake of intelligent end-user devices have transferred many key functionalities to the edge of the network resulting in end-users having much more access to, and control over, what were traditionally network functions. This has been a welcome development for the vast majority of end-users in terms of choice and access to applications and services but the negative impact is that it has also made fraud and misuse much easier to perpetrate and it is now a global problem.

Technological developments have also enabled an ecosystem for electronic communications which is borderless and this, again while beneficial for end-users, has created jurisdictional problems for law enforcement authorities to prosecute those who perpetrate fraud on victims in one country from another country. Initiatives for international cooperation have been implemented, for example at ITU level, but in the absence of more robust arrangements and global techniques to tackle fraud and misuse it will continue to be a problem.

The following sections of this chapter examine measures taken at the national level in CEPT countries to tackle fraud and misuse. In order to inform this report, the ECC conducted a survey of CEPT member countries to gather information on the different approaches employed to tackle fraud and misuse where E.164 numbers play a role. Responses from 17 CEPT countries were received and the results are summarised below.

5.1 DEFINING FRAUD

Some respondents to the questionnaire stated that they do not have specific definitions for fraud involving E.164 numbers. One country referred to the Global System for Mobile Communications Association or GSM Association (GSMA) categories of fraud, namely: Subscription fraud, technical fraud, distribution fraud, business fraud and prepaid fraud. Some respondents did provide specific definitions which are summarised below:

- Any misleading action related to access to numbers and/or services performed for profit or receiving a benefit at the expense of end users;
- The sending, routing or receipt of text messages or multimedia messages or making, routing, or receipt of calls using services or numbering intended for an end-user as a result of which useless or artificial traffic arises which may express as uniform calls in duration of connection or as calls, text messages, multimedia messages in an uncharacteristic amount for a user, which are made by an end-user or equipment connected to a termination point existing in the country or outside the country;
- Irregular traffic for fraudulent purposes: Traffic that is generated, induced or artificially prolonged in order to obtain profit, direct or indirect, from the payments chain. This definition has been set out in national legislation.

For the purposes of developing a report [9] on cross-border issues related to Article 28(2) of the USD, BEREC defines fraud as follows: *"Any deceitful practice with cross-border impact perpetrated for profit or to gain some unfair or dishonest advantage over end-users of electronic communications services"*.

5.2 DEFINING MISUSE OF E.164 NUMBERING RESOURCES

Two respondents to the questionnaire stated that they do not have specific definitions for misuse of E.164 numbers but define misuse in analogy with the definition specified by the ITU. According to ITU-T

Recommendation E.156[4,] misuse of an international E.164 numbering resource occurs *"where the use of that numbering resource does not conform to the relevant ITU-T Recommendation(s) assignment criteria for which it was assigned or when an unassigned numbering resource is used in the provision of a telecommunication service".*

The BEREC Report (referred to in Section 5.1 above) defines misuse as *"use of numbering resources in an unauthorised way, which may cause harm to end-users of electronic communications services and with cross-border impact".*

Respondents to the ECC questionnaire provided the following definitions of misuse of E.164 numbering resources as follows:

- *"Use of numbers not for their designation when it results in harm to end-users and/or businesses. This definition is set out in national guidelines";*
- *"Use of numbering not corresponding to the purpose of use of numbering determined in the national numbering plan, as well as initiation, routing or receipt of calls to national numbers that have not been activated or used in the public telephone network in the country, or to a number of the public mobile telephone network which is not used for terminal equipment connection of an end-user in the public telephone network of an electronic communications merchant in the country, except roaming in the public mobile telecommunications network. This definition is set out in national legislation";*
- *"Misuse due to the use of unauthorised numbering resources: The use of national or international public numbering resources that have not been allocated or assigned. This definition has been set out in national legislation";*
- *"Misuse due to the improper use of numbering resources: The use of public numbering resources that have been assigned but used contrary to the established provisions of attribution, authorisation or application. This definition has been set out in national legislation".*

5.3 DEFINING CLI SPOOFING

ECC Report 248[5] defines CLI Spoofing as *"a procedure that enables the calling party to manipulate the information displayed in the CLI field so that the called party thinks that the call originates from another person, entity or location".*

Only one respondent to the questionnaire provided a definition of CLI spoofing while others provided information on the general rules governing CLI in their respective countries. The definition provided is as follows: *"To make receiving terminals display a manipulated address, such as a phone number or name, that does not identify, for the called party, who is calling".*

For the purposes of this report, an amended version of the definition provided in ECC Report 248 has been used. It defines CLI spoofing as "a technique that enables the calling party to manipulate the information displayed in the CLI field *with the intention of deceiving* the called party in to thinking that the call originated from another person, entity or location". CLI spoofing can also be carried out by originating and transit operators.

The purpose of adding the words "with the intention of deceiving the called party" is to emphasise that the intention of manipulating the CLI is malicious when fraud or misuse is perpetrated given that fraud and misuse are the subject of this report. ECC Report 248 describes certain scenarios where there may be a consumer benefit of being able to manipulate CLI information under certain conditions.

[4] ITU-T Recommendation E.156 Guidelines for ITU-T action on reported misuse of E.164 number resources – May 2006 https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.156-200605-I!!PDF-E&type=items

[5] ECC Report 248 - Evolution in CLI usage – decoupling of rights of use of numbers from service provision – April 2016 https://www.erodocdb.dk/download/06aa677b-7481/ECCRep248.pdf

5.4 NATIONAL LEVEL INITIATIVES

Generally speaking the detection and prevention of any kind of fraud is a matter for the national law enforcement authorities. In most CEPT countries the NRA or the competent telecommunications authority will either have a limited formal role or no formal role whatsoever in tackling fraud. When it comes to telecoms fraud the NRA or the competent telecommunications authority cooperates with the national law enforcement authorities, usually on an informal basis. At least 4 CEPT countries have either established working groups or technical committees to tackle the issues of fraud and misuse of E.164 numbers. In one case a working group was established to work out measures in order to mitigate and stop fraud, misuse and spoofing. One of the initial outcomes was the creation of an information system (via email) to quickly share information between operators on specific fraud cases. This gives operators useful information to take decisions on necessary measures such as blocking suspicious or fraudulent traffic. Committees or working groups have also been established to facilitate cooperation between relevant national authorities to tackle fraud and misuse. One country has created a database that contains information on reported instances of fraud. In one country which has developed specific regulations to tackle misuse and fraudulent traffic on Electronic Communication Services (ECS), operators whose technical criteria for identifying such traffic have been approved by the competent telecommunications authority can automatically block traffic and withhold payments at national level.

In relation to misuse of E.164 numbers specifically, NRAs or the competent telecommunications authorities have normally a more formal role. The NRA may take measures to remedy misuse to secure compliance with national numbering legislation including issuing orders for blocking traffic, withholding payments and, where fraud occurs in conjunction with misuse, imposing fines on guilty parties. However, where remedies exist in law it may not always be possible for the NRA or the competent telecommunications authority to invoke them. For example in one CEPT country there is a provision in the legislation for the NRA to impose fines on guilty parties but the NRA lacks the necessary means and powers to do so. In particular, it does not have the power to investigate and thus detect the person responsible. This would require gaining insight to electronic communications traffic data which would contravene national legislation on privacy.

Several respondents to the questionnaire provided information on the rules around CLI in their respective countries. While only 8 of the CEPT countries surveyed explicitly forbid CLI spoofing in national legislation there is a general rule across all CEPT countries that only the originating line or access (e.g. geographic, mobile and nomadic numbers) identifiers can be used as CLI. Certain exceptions are made in many countries which require regulatory approval on a case-by-case basis. For example, in some cases, the use of some short numbers, freephone numbers and a geographic number from a mobile access in FMC services as CLI has been authorised following requests from service providers. The use of premium rate services numbers as CLI is forbidden in most CEPT countries. Furthermore, the use of a CLI in alphanumeric format is also generally permitted for messaging services provided it denotes the calling party in question.

Therefore, and considering whether CLI spoofing is explicitly forbidden or not, there have only been a few initiatives aimed at tackling the problem.

In at least one case an existing working group on numbering established guidelines for CLI. These guidelines include a list of basic principles that aim to ascertain the industry's responsibility to facilitate that the number that best indicates the real caller should be presented to the call recipient and numbers that cannot be directed, including numbers that are not assigned, should not be presented as CLI. In response to a number of cases where CLI spoofing facilitated fraudulent activity, the national directory enquiry services received a surge in enquiries on specific numbers. This information was shared with the NRA who collected the affected numbers in a database and provided the information to the operators. It was then up to the operators to take measures they deemed necessary to resolve the problem.

Finally, it is often the case that when CLI spoofing occurs the calls are originated outside of the national territory thereby making jurisdiction a problem. One country attempted to contact the NRA of another country outside of the CEPT area to seek cooperation on resolving the problem. This has proven to be unsuccessful to date.

6 MEASURES IMPLEMENTED IN THE US TO TACKLE FRAUD AND MISUSE OF E.164 NUMBERS AND CLI SPOOFING

6.1 US BILL ON CLI FALSIFICATION:

Under the Truth in Caller ID Act of 2009 [10], FCC rules prohibit any person or entity from transmitting misleading or inaccurate Caller ID information with the intent to defraud, cause harm, or wrongly obtain anything of value. If no harm is intended or caused, spoofing is not illegal. Anyone who is illegally spoofing can face penalties of up to US$10,000 for each violation. In some cases, spoofing can be permitted by courts for people who have legitimate reasons to hide their information, such as law enforcement agencies working on cases, victims of domestic abuse or doctors who wish to discuss private medical matters.

On 22 June 2011 the FCC issued the rules and regulations implementing the Truth in Caller ID Act of 2009 and submitted its report on Caller Identification Information in Successor or Replacement Technologies [11]. The FCC examined the Caller ID aspects of technologies underlying current trends in communications and submitted legislative recommendations to tighten the current prohibitions on malicious Caller ID spoofing and to address identification spoofing in new and emerging communication services. Legislative recommendations also include clarifying the scope of the Truth in Caller ID Act to include (1) persons outside the United States, (2) the use of Internet Protocol (IP)-enabled voice services that are not covered under the Commission's current definition of interconnected Voice over Internet Protocol (VoIP) service, (3) appropriate authority over third-party spoofing services, and (4) SMS-based text messaging services.

The rationale for making caller identification spoofing illegal was the observation that applications of such an activity are usually for malicious purposes.

6.2 ROBOCALLS AND TELEMARKETING CALLS

Although unwanted robocalls and telemarketing calls are not within the scope of this report there is some interference with misuse and fraud involving E.164 numbers. It is also useful to learn on how this problem is approached in the US.

As stated in the Robocall Strike Force Report [12], October 26 2016 *"Robocalls and telemarketing calls are currently the number one source of consumer complaints at the FCC. The FCC has been encouraging service providers to offer call blocking solutions that give customers greater control over the types of calls they receive. Call blocking is one part of the robocall solution. Another part is identifying the bad actors who use robocalls to take advantage of unsuspecting consumers by using numbers assigned to others (spoofing). They use cheap and accessible technologies to spoof their caller identity and scam victims".*

The Robocall Strike Force was created on request of the FCC where the industry was given the responsibility to come up with solutions to stop unwanted robocalls and telemarketing calls.

Three lines of action were identified in order to successfully stop or reduce illegal robocalls and telemarketing calls: 1) source identification, 2) network and consumer blocking tools, and 3) effective enforcement with the power to traceback and shut down offenders.

It was also noted that just as with any other types of fraud and misuse a diverse multitude of evolving mitigation tools and efforts will be needed so that it becomes too costly for illegal robocalling campaigns to overcome the industry's dynamic mitigation techniques.

6.2.1 Source identification

Offenders can easily spoof E.164 numbers and hide their identity which contributes to the proliferation of illegal robocalls and marketing calls. In order to remove this "opportunity" work has started within the Internet Engineering Task Force (IETF) to develop the standards to verify and authenticate caller identification for calls carried over an Internet Protocol (IP) network. These standards are known as SHAKEN (Signature-based Handling of Asserted information using tokens) and STIR (Secure Telephony Identity Revisited)6.

The premise of STIR/SHAKEN is that telephone calls and the telephone numbers associated with the calls, when they are originated in a service provider network can be authoritatively and cryptographically signed by the authorized service provider, so that as the telephone call is received by the terminating service provider, the information can be verified and trusted.

The protocols and specifications defined in the IETF STIR working group form the basis of the SHAKEN industry framework. This set of industry standards is intended, as it is more fully deployed into the VoIP based telephone network, to provide a basis for verifying calls, classifying calls, and facilitating the ability to trust caller identity end-to-end. Illegitimate actors can then be more easily and quickly identified with the hope that telephone fraud is reduced significantly.

Further it is noted that carriers are at various stages of transitioning to IP-enabled networks and SHAKEN fundamentally depends upon IP network technologies.

6.2.2 Network and consumer blocking tools

Basically end-users should be empowered to better control their communications. That means that they should be given a greater degree of identification and control over the types of calls they receive.

A need was identified to develop information flows, consumer presentation and consumer-directed call disposition control options. These will give consumers a clearer picture of the type of calls they are receiving, and expand their automatic and manual call handling options.

The US industry has been considering how verified Caller ID information can and should be displayed on a user's wireless handset to enable real time decision making by consumers about incoming calls. Questions include whether there should be standardisation with respect to a minimum set of display requirements or whether that is best left to the network, Original Equipment Manufacturer (OEM) and "app" communities.

6.2.3 Detection, Assessment, Traceback, and Mitigation

The US industry investigated various methods of detection and avoidance to stop unwanted calls from reaching customers by blocking at various network levels. Also a trial has started to block known numbers that should never originate traffic. The results of this trial will help determine the viability and effectiveness of a "Do Not Originate" list of numbers to be blocked network wide in the future.

Also work was done by the operators with the goal of easing and simplifying the process of tracing the origins of robocalls, otherwise known as "traceback". During the course of these efforts, the operators noted that the sharing of certain network intelligence and traceback information among its participants could and did lead to the successful thwarting and mitigation of unwanted and illegal phone traffic.

A key lesson learned from the US industry’s extensive experience and leadership in traceback efforts is that with investments in personnel and IT systems, along with providers’ contact information for traceback and subpoena requests being readily available, voice providers can establish the systems and processes needed to efficiently process requests (whether government subpoenas or requests from other carriers) to identify the source of suspicious traffic traversing their networks.

It was also considered beneficial to include service providers from outside of US in these robocall mitigation efforts. Therefore a framework was developed for participation and governance.

[6] These standards are not applicable in non-IP networks (e.g. PSTN, 3G)

7 PREVENTION, DETECTION AND ADEQUATE RESPONSE VIA TECHNICAL MEASURES

7.1 WANGIRI (OR PING CALLS)

In order to counter ping calls (also this applies for voice spam - see ITU-T Recommendation X.1246) network-side technologies or user-side technologies can be used. Both are complementary but the user-side technology is more customisable.

7.1.1 Network-side technologies

In order to detect ping calls in the first step the signalling information of incoming calls has to be collected online. Based on this information an analysis can be made to identify suspicious calls based on some characteristics such as call frequency, connection rate, ring tone duration and existing blacklists. The analysis can take place in real time or almost real time. The outcome of the analysis has to be verified before action can be taken by the operator's fraud department. If the verification process is passed the CLI is put on the blacklist and incoming calls with a CLI on the blacklist are blocked. If it is not possible for an operator to block a call, another option is to hide the CLI: the user will receive the call but, since the CLI is not displayed, the user will not be able to call back.

The blacklists can be shared between operators if they collaborate. The NRA or competent telecommunications authority can play a role in coordinating this process. Blacklists inevitably contain inaccuracies that prevent legitimate calls to pass. In such cases, a process is required in order to be able to remove a number from the blacklist.

7.1.2 User-side technologies

Users can install on their smartphone certain applications in order to block numbers used for initiating ping calls. On certain devices this is already foreseen as standard. If they receive ping calls they can add the number to the application and refuse the call or divert it to voice mail. Also some databases with blacklists exist, but the application requires a data connection to access these.

Examples of smartphone apps include:

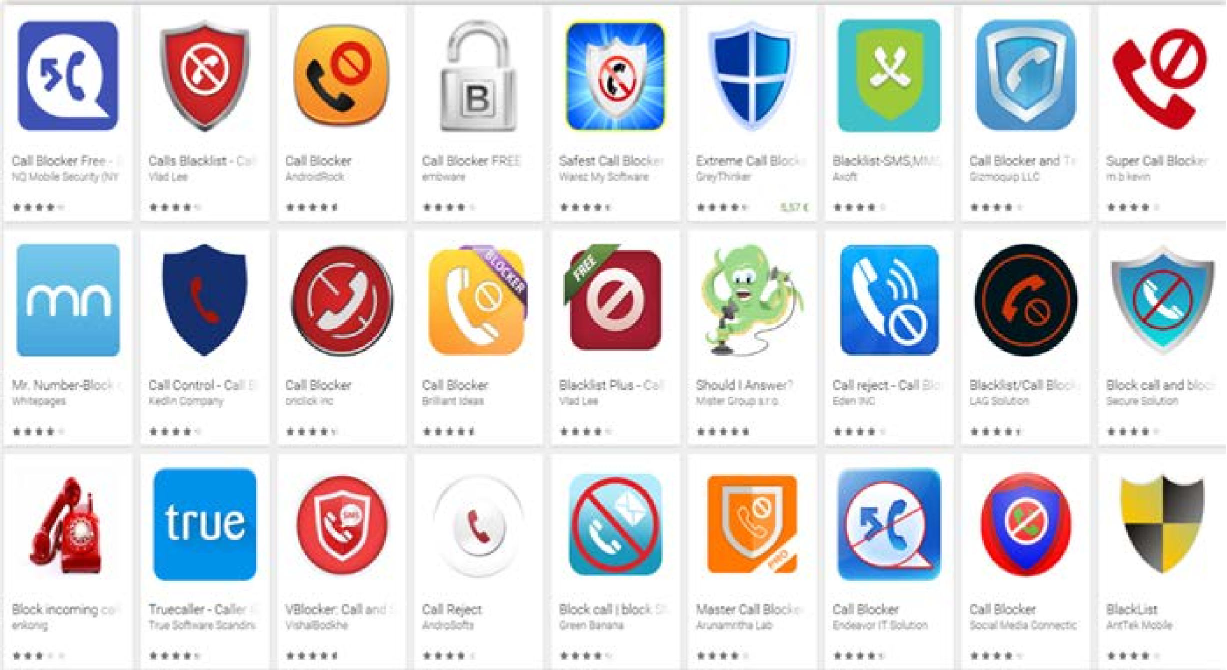


Figure 3: Examples of call blocking apps

7.2 CALL HIJACKING AND SHORT STOPPING

Call hijacking and short stopping can be difficult to detect without reports from end-users complaining that the calls are not reaching the defined destination. With short stopping, if the operator has several years of statistics for its customers calls to premium rate numbers in defined destinations, it is possible to analyse the situation where the number of such calls rapidly increases. Operators should also be cautious when preparing bills for end-users because end-users will complain if charged for calls to premium rate or other high tariff numbers they are unaware of.

Usually the investigation starts with the originating operator asking the transit operator with which it has an agreement regarding the destination and call path used to terminate the call.

The role of the NRA or competent telecommunications authority in the destination country in the investigation is limited, because the authority can only provide the information to which operator the number ranges were assigned. Authorities could play a more effective role if transit operators are located within their jurisdiction in cases where transit operators do not want to give information or the information is not trustworthy. The authorities in the originating country can also play a role, for example, by instructing the blocking of traffic and/or the withholding of payments between international operators even if it is difficult to impose these kinds of measures.

If such types of fraud and misuse like call hijacking and short stopping where artificial traffic is not used (normally the real traffic is used), it is not possible to completely prevent call hijacking and short stopping. To minimise the number of cases of call hijacking and short stopping, the operators should be cautious, if inadequate low prices are offered by the transit operator for call transit and/or call termination for the traffic routing to defined destination. It is recommended for operators to use services of well-known transit operators.

7.3 HIGH TARIFF NUMBERS

High tariff or premium rate E.164 numbers are especially vulnerable to being taken advantage of for fraudulent purposes. International Revenue Share Fraud (IRSF) is the top ranking type of telecom fraud worldwide, according to a 2017 report [13] by the Communications Fraud Control Association (CFCA). The worldwide losses caused by IRSF – in 2017 estimated to be US$6.1 billion – is almost 50% more than that caused by the second ranking type of fraud (interconnect bypass) which is estimated to be US$4.27 billion.

As explained earlier in this report, IRSF is conducted through different techniques where the goal of the fraudulent party is to initiate unauthorized calls to high tariff or premium rate E.164 numbers and make the calls last for as long as possible. Most premium rate number products are simple, with only a so-called IVR system playing a message customized by the subscriber. However, there is no need to play a message for completing fraudulent calls. The financial incentive driving this type of fraud and misuse is the pay-out received from the company using the number(s) in question ("kickback"). An important facilitating factor for IRSF is the money flow via the interconnect agreements between the operators in the chain.

According to the CFCA report, the top five countries where fraudulent calls terminate are Cuba, Latvia, Lithuania, UK and Tunisia. The top five countries where fraudulent calls originate are the United States, Spain, UK, Russia and Palestine. The termination point needs to be placed in context however as not all frauds would have been traced by their true termination. It may be perhaps more accurate to state that these calls terminate on numbers belonging to the national numbering plans of these countries. The CFCA report also notes that global telecom fraud decreased 23.3 % (from over US$38 billion to US$29.2 billion) since the last global fraud loss survey (2015). However, with losses of US$ 6.1 billion through IRSF alone, telecom fraud is still a problem that must be addressed. The ECC, in its discussions with some industry players, notes that the numbers of complaints from operators about fraud are increasing. Therefore, telecom fraud is still a problem that must be addressed.

As mentioned above, the financial incentive behind IRSF is the pay-out received by generating calls to high tariff or premium rate E.164 numbers. Due to the presence of many premium rate service providers competing with attractive pay-outs and uncomplicated terms, the "business model" of IRSF is made lucrative and rather undemanding to implement for those with the desire to commit fraud. This conclusion is made in a 2015 white paper [14] published by TransNexus, a software development company specialising in applications for managing wholesale VoIP networks.

The above-mentioned report also concludes that the typical premium rate service provider is a small "virtual" company, often with no disclosed location or contact number, only communicating via e-mail. TransNexus found that the UK and the US have the highest concentration of premium rate service providers. However, as many such providers do not disclose their location the actual situation may be different.

The TransNexus report also identifies the top ranking destinations for IRSF risk. Based on highest pay-out, the top six are five countries and one global satellite network: UK, Austria, Estonia, Inmarsat, Latvia and Oman.

According to TransNexus, "the eco-system needed to monetize IRSF is thriving". The question is which measures can be used to hinder and minimize fraud and misuse with high tariff or premium rate E.164 numbers.

Operators should invest more in sophisticated call monitoring systems which in an early phase can, based on data analytics, detect suspicious traffic. To make such systems effective and efficient especially traffic to numbers with high termination rates or countries which are known as being problematic for fraud or misuse should be monitored. Therefore, it seems to be useful to create more transparency in the numbering plans and associated services of all countries.

Once suspicious traffic is detected operators should, on their own initiative after further analyses, block the number ranges used for fraud or misuse. A mechanism has to be foreseen to open these numbers again if the risk on fraud or misuse disappears. It can be useful to share information between market players on numbers which are fraudulent or misused.

8 DUTY OF CARE

In order to propose effective and efficient measures to be implemented for minimising fraud and misuse of E.164 numbers it is necessary to study the roles and responsibility of the different operators in the value chain. In order for end-users to make and receive communication and enable access to services in such networks, interconnection between the originating network operator and the terminating network operator is required. Sometimes also a transit network operator is involved. In this section, the role and responsibility and what can be reasonably expected from each of the different operators ("duty of care") is described. Also reasonable expectations foreseen for end-users are described.

Duty of care goes further than just acting according to the law. It is expected that operators, if they have knowledge that misuse or fraud is directly or indirectly taking place using their networks, follow ethical standards and take action in a proportionate way. This is very similar to what exists in the hosting sector. Hosting sites can only claim the liability exemption as long as they do not have knowledge of the illegal nature of the content and they perform their duty of care. This implies that if they are notified they will have to remove or block the content and that they can be subjected to monitoring obligations. The E-Commerce Directive [15] mainly encourages self-regulation and co-regulation but also leaves some space for Member States to impose specific monitoring obligations and duties of care as well as creating a notice-and-takedown procedure.

When describing what can be reasonably expected and what measures can be taken from the different operators in order to minimise fraud and misuse it is important to acknowledge that taking measures is a cost factor. The benefit of keeping customers safe should also be acknowledged as it is in the interest of the operators to protect their customers. Otherwise the operator's reputation will be damaged, which can have significant cost implications.

8.1 ORIGINATING AND TERMINATING NETWORK OPERATOR

Call origination is the beginning of a call made by an end-user. The call originates in the network belonging to the network operator to which the calling party is connected or has a subscription. Call termination is the end of a call made by an end-user. The call terminates in the network belonging to the network operator to which the called party is connected or has a subscription.

If originating and terminating operators have knowledge that their users are subject to fraud or misuse (e.g. wangiri fraud) they should block, without delay, these incoming and outgoing calls without legal order. These operators should continue to invest in sophisticated antifraud detection systems and offer that to their customers.

8.2 TRANSIT NETWORK OPERATOR/WHOLESALE OPERATORS

Between the originating and the terminating network a transit network is usually involved for international/cross border calls. A transit network bridges a connection between the originating and the terminating network.

Historical contracts of wholesale operators do not foresee any fraud management measures and as such foresee payment in all cases. In the last 3 or 4 years this changed following a shift in the market and a greater willingness of some carriers to help fight against fraud. In new contracts provisions such as *“neither party shall be obliged to establish a credit note for the supply of a carrier service for which the other party could not collect the corresponding amount with its end-user (e.g. in the event of insolvency or fraud)”* are increasingly being included.

But the value of such legal clauses (detailed or high level) is limited as the market has not the same maturity level in all regions of the world and is not symmetric when it comes to fighting fraud (depending if an operator is a victim or benefits from it). Thus, such contractual clauses remain "best effort" whenever they are accepted. In practice the fight against fraud remains best effort also due to the fraud definition gap between international carriers linked to different laws and regulations in each country. European wholesale operators should continue to increase their efforts to include antifraud clauses in their interconnection agreements with partners both within and outside of Europe.

International carriers (and others) are developing products for fraud prevention (CLI reliability scoring, A-number barring etc.) for traffic passing over the different network borders. Such initiatives should be encouraged.

8.3 USERS

Reasonable expectations are not only relevant and foreseen for the different operators. There are also reasonable expectations foreseen for end-users. End-users need to be aware and take a critical look when calls, SMS and social media messages are received. Initiatives to raise awareness and educate end-users as to the dangers of fraud and misuse and how to deal with such communications need to be implemented. In relation to WAP billing, end-users should be vigilant and ensure that they pay careful attention to any additional charges on their telephone bills.

Also end-users play a role in relation to the discovery, investigation and prosecution of fraudsters. If experiencing fraud and misuse cases end-users should report such cases to their service provider, the national police and/or relevant authority. Simple reporting mechanisms should be created and implemented for end-users if they are faced with fraud and misuse.

9 COMPETENCE ISSUES

As described above there are different types of fraud and misuse involving E.164 numbers using different technologies and for different purposes. In most CEPT countries it is the law enforcement authorities that have competence to tackle fraud and NRAs or the competent telecommunications authorities may only be involved in an informal way in assisting with the investigation of fraud schemes as described in this report. However, in some CEPT countries the NRA may to some extent be involved. The division of competence between national authorities depends on the legal situation in each country.

Usually, the type of fraud and misuse described in this report is in the competence of criminal law enforcement (the police and courts). This is particularly the case if the purpose of the fraud or misuse is a financial gain or identity theft. Other types of misuse or parts of the fraud may be in the competence of the NRA or the competent telecommunications authority.

Due to the characteristics of the fraud and misuse where in most cases victims do not file a complaint because the monetary loss is low or not existing, e.g. if the purpose of the misuse is "only" harassment and taking into account the often international character it is extremely difficult to find and prosecute the fraudsters. It is very difficult, if not impossible, to completely stop this fraud or misuse via the normal judicial system.

Even if NRAs or the competent telecommunications authorities are not directly competent for or involved in the investigation of fraud and misuse NRAs or the competent telecommunications authorities can take measures to ensure, to the extent possible in their policy and legislation, that numbering resources are not facilitating fraud and misuse. Also, NRAs or the competent telecommunications authorities can assist the police and courts with their technical knowledge during the investigation and prosecution of fraud and misuse cases.

10 INTERNATIONAL COOPERATION

ITU-T WTSA Resolution 20 [16] has noted that it is in the common interest of ITU-T Member States and Sector Members that the recommendations and guidelines for international telecommunication numbering, naming, addressing and identification resources should be known, recognized and applied by all and used to build and maintain confidence of all in the related services. For that reason a procedure [5] guiding ITU-T Member States and Sector Members to report misuse of numbers was produced.

Based on this procedure, ITU-T developed a database[7] containing all the reported cases of misuse. In the beginning this database included only a few notifications. Nowadays the number of notifications has increased significantly. However, the number of notifications made might only represent very low percentage of the existing misuse cases.

The sharing of intelligence on fraud and misuse at conferences directly between experts must be encouraged. NRAs or the competent telecommunications authorities should also take part in such a process as the fight against fraud and misuse can only be won if all involved stakeholders closely collaborate.

[7] https://www.itu.int/net/ITU-T/misuse/table.aspx - Access is only possible by a TIES user

11 RECOMMENDATIONS FOR BEST PRACTICES

In order to tackle fraud and misuse effectively a holistic approach that takes into account the dynamic character of fraud and misuse is needed. Although the focus of this report is voice, fraud and misuse in telecom is of course not limited to voice. SMS and social media messaging are also vulnerable to fraud and misuse.

The following recommendations are made:

11.1 PROHIBIT CLI SPOOFING

Clear regulatory guidelines and technical standards on CLI should be set. As CLI spoofing is increasing and is used as a means to facilitate misuse and fraud it is important to explicitly state in the law that such a practice should be forbidden for calling parties and originating and transit operators. A careful formulation of such an instrument is needed as in some exceptional situations manipulating CLI information is acceptable, e.g. for law enforcement officials or other people in order to protect their privacy, as long as it denotes the calling party in question and no other entity (whether in numeric or alphanumeric format) and as long as it does not denote a premium rate number enticing call back. These regulatory guidelines should also provide operators with a clear and transparent legal context to take appropriate actions in case of fraud and misuse.

Technical standards need to be developed and implemented globally to verify and authenticate caller identification for calls carried over IP-based networks. The initiatives taken by the SIP Forum, by using a digital certificate scheme, and by the IETF with its ongoing work on the SHAKEN and STIR standards, are positive steps. However in order for these standards to be effective in combatting international CLI spoofing they need to be implemented on a global scale, with the implications that follow in terms of timetable, costs and coordination.

In order to maintain integrity and trust in E.164 numbers and Calling Line Identification (CLI), validation techniques as described in ECC Report 248 should be implemented. The validation should be made periodically in order to prevent the number being used by two different end-users at the same time when the number is re-assigned to a new end user by the original provider.

11.2 DUTY OF CARE

European operators should continue to increase their efforts to include and enforce antifraud clauses in their interconnection agreements with partners within and outside of Europe. Operators should also actively develop and apply sophisticated fraud management systems. In relation to WAP billing, operators should explore the possibility of using alternative identifiers in the HTTP header for WAP billing as using the end user's telephone number raises privacy concerns.

11.3 ENCOURAGE REAL TIME DATA ANALYTICS

Operators will increasingly have to invest in solutions that facilitate intelligent real time data analyses of call detail records and signalling messages. These analyses must result in the detection of patterns of calls which are suspicious while at the same time trying to minimise false positives. Based on the results of these sophisticated analyses swift and effective action must be taken to minimise the impact on revenues and end-user welfare.

11.4 PROMOTE INFORMATION SHARING AND COOPERATION

Once an instance of fraud or misuse is detected it can be beneficial to share related information between operators and other relevant stakeholders. NRAs or the competent telecommunications authorities can steer this process as it can only work if confidence is created between the stakeholders and information is shared based on a mutual collaboration to tackle fraud and misuse.

The information sharing includes information on specific cases (e.g. suspicious numbers), fraud and misuse methods or even the modus operandi of certain stakeholders in the value chain. The information sharing should not only take place at the national level but also at the international level (e.g. by creating a worldwide network of contacts). Easy blocking mechanism for incoming and outgoing traffic

Operators should have some discretion to create simple and quick internal procedures to block incoming and outgoing calls which are fraudulent or involve the misuse of E.164 numbers without any intervention of a court order or NRA or the competent telecommunications authority.

11.5 ESTABLISH STANDARDISED PROCEDURES FOR TRACE BACK CALLS/TEST CALLS

For serious and large scale fraud, easy procedures should be created in order to facilitate an expeditious trace back of calls across national borders. Requirements to this effect could be included in interconnection agreements to facilitate detection of the sources of fraud.

11.6 TRANSPARENCY

A central reference point for national numbering plans[8], which clearly identifies mobile, premium and unassigned E.164 number ranges, could create the necessary transparency to flag possible problematic calls and routes. Based on that information a list can be made of expensive number ranges which are vulnerable to fraud or misuse and which can be used as an input in the data analytics systems.

11.7 RAISING AWARENESS

End-users need to be aware and take a critical look when calls, SMS and social media messages are received. Initiatives to raise awareness and educate end-users as to the dangers of fraud and misuse and how to deal with such communications need to be implemented. Simple reporting mechanisms for reporting fraud and misuse to the national police and/or competent authority should be implemented. In relation to WAP billing, end-users should be vigilant and ensure that they pay careful attention to any additional charges on their telephone bills.

[8] ITU-T is currently examining the feasibility of a database containing information on all national numbering plans

ANNEX 1: LIST OF REFERENCES

[1] The Adaptive Mobile Blog - Article on Wangiri Fraud in Ireland - https://www.adaptivemobile.com/blog/irelands-call-careful-now

[2] ECC Report 133 - "Increasing Trust in Calling Line Identification and Originating Identification"

[3] ECC REC (11)02 - Calling Line Identification and Originating Identification"

[4] ECC Report 248 - "Evolution in CLI usage – decoupling of rights of use of numbers from service provision"

[5] ITU-T Recommendation E.156 - "Guidelines for ITU-T action on reported misuse of E.164 number resources"

[6] ITU-T Recommendation E.157 - "International calling party number delivery"

[7] ITU-T Recommendation E.164 - "The international telecommunication numbering plan"

[8] "Article 28(2) USD Universal Service Directive: A harmonised BEREC cooperation process - BEREC Guidance paper" (7 March 2013)

[9] BEREC report BoR (10) 62 Rev1 on cross-border issues under Article 28(2)USD – February 2011 - http://berec.europa.eu/doc/berec/bor_10_62Rev1.pdf

[10] Truth in Caller ID Act of 2009. Available at: https://www.congress.gov/bill/111th-congress/senate-bill/30

[11] FCC Report on Caller Identification Information Successor or Replacement Technologies pursuant to the Truth in Caller ID Act of 2009. Available at: https://apps.fcc.gov/edocs_public/attachmatch/DA-11-1089A1.pdf

[12] Robocall Strike Force Report, 0ctober 26, 2016. Available at: https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf

[13] CFCA_Global_Fraud_Loss_Survey_2017 - Available at: www.cfca.org/fraudlosssurvey/

[14] 2015 white paper "The International Premium Rate Number Market" published by TransNexus. Available at: http://transnexus.com/resources/white-papers/international-premium-rate-number-market

[15] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

[16] Resolution 20 (Rev. Hammamet, 2016) - Procedures for allocation and management of international telecommunication numbering, naming, addressing and identification resources

[17] ECC REC (07)02 - "Consumer Protection Against Abuse of High Tariff Services"

[18] ECC Report 86 - "Consumer Abuses and Fraud Issues Related to High Tariff Services"

[19] ECC REC (05)09 - "Customer Protection in Case of Misuse or Unauthorized Use of International E.164 Numbering Resources"