



ECC Newsletter May 2019

## Intelligent Transport Systems

Two recently published CEPT Reports set out the spectrum parameters that will facilitate safer and more effective intelligent transport systems in the future

The development of connected and autonomous vehicles has had a further boost after the Electronic Communications Committee (ECC) approved two CEPT Reports that will facilitate their development. At its 50th meeting, which was held in Brighton in the UK from 4-8 March, the ECC approved:

- CEPT Report 70 in response to the permanent European Commission (EC) Mandate on Short Range Devices (SRDs). This Report contains a range of proposals to assist in the seventh update of the SRD Commission Decision. Amongst these is the proposal of two initiatives which are intended to help drive innovation in the automotive sector and to improve the safety of road vehicles.
- CEPT Report 71 in response to the EC Mandate to CEPT to study the extension of the Intelligent Transport Systems (ITS) safety-related band at 5.9 GHz. This Report proposes extending the upper edge of the EC harmonised safety-related ITS band (5875-5905 MHz) by 20 MHz up to 5925 MHz. In addition, it proposes to harmonise the frequency band 5925-5935 MHz for safety-related Urban Rail ITS applications.

### CEPT Report 70

CEPT Report 70 makes two proposals for Transport and Traffic Telematics (TTT).

First, the Report suggests widening the frequency bandwidth in the 60 GHz range from 63-64 GHz to 63.72-65.88 GHz. This would facilitate TTT to better align with the channelisation of wideband data transmission systems operating in the 57-66 GHz range. The power limitation remains unchanged at 40 dBm e.i.r.p. This improvement is described more fully in the draft ETSI Systems Reference Document (SRDoc) on the technical characteristics of Multiple Gigabit Wireless Systems (MGWS) in radio spectrum between 57 GHz and 71 GHz (TR 103 583). This draft SRDoc notes that the current 63-64 GHz ITS allocation overlaps two of the MGWS channels, specifically Channel 3 and Channel 4.

Shifting the CEPT allocation so that it only overlaps with a single channel would significantly enhance sharing operation. The shift and the combined increase of the allocated spectrum will allow ITS applications to take advantage of existing MGWS technology. This will greatly reduce both cost and deployment time for ITS applications. ETSI is currently developing the necessary equipment standards for ITS in this revised frequency band.

Second, the Report suggests allowing smart tachograph – the new generation of on-board digital recorders – in the frequency band 5795 to 5815 MHz, as set out in the table below.

Frequency Band	Category of Short Range Device	Transmit Power Limit	Additional parameters (channelling and/or channel access and occupation rules)	Other usage restrictions
5795-5815 MHz	Transport and Traffic Telematics devices (TTT)	2 W e.i.r.p.	Techniques to access spectrum and mitigate interference that provide at least equivalent performance to the techniques described in harmonised standards adopted under Directive 2014/53/EU must be used.	This set of usage conditions applies only to road tolling applications and smart tachograph, weight and dimension applications.

Smart tachograph, weight and dimension applications are defined as "remote enforcement of the tachograph in Appendix 14 of the Commission Implementing Regulation 2016/799 and for the weights and dimensions enforcement in Article 10d of EU Directive 2015/719".

The regulations allow for the use of an interrogator device called a Remote Early Detection Communication Reader (REDCR). There are two use cases for this technology:

- The in-vehicle unit is read out by a fixed or portable REDCR located at the roadside which is directed towards the centre of the windscreen of the passing vehicles it wants to inspect.
- The in-vehicle unit is read out from a mobile REDCR situated within a moving vehicle and directed towards the centre of the windscreen of the vehicle it wants to inspect.

This technology will allow road enforcement authorities to interrogate the tachograph unit on the commercial vehicle. There are clear benefits for safety in allowing police forces to read tachograph information without the need to pull over each vehicle of interest.

The original compatibility analysis can be found in ECC Report 291 - Compatibility studies between smart tachograph, weight and dimension applications and systems operating in the band 5795-5815 MHz and systems operating in adjacent bands.

ETSI EN 300 674 for TTT will be the applicable harmonised standard for smart tachograph, weight and dimension applications.

## CEPT Report 71

CEPT Report 71 suggests significantly increasing the radio spectrum available for safety-related ITS systems. In February 2017 the Radio Spectrum Policy Group (RSPG) delivered its opinion on spectrum aspects of ITS which states that "there is no evidence that spectrum availability is currently a constraint on the development of ITS, and there is no immediate need to take regulatory action in this regard. However, given the momentum of policy and standardisation development for ITS, we recommend that the options for ITS to expand to share spectrum for safety-related ITS in the 20 MHz above the existing designation and, for non-safety-related ITS, in the 20 MHz below, should be kept available for the time being. It is also important to take into account the developments in ITS technologies and the introduction of Communication Based Train Control (CBTC) within the ITS designation".

CEPT considers that its Report satisfies the RSPG opinion of 2017 and that it can be used as a basis for the amendment of EC Decision 2008/671/EC on safety-related ITS.

Since the introduction of the current ITS regulations in Europe, new technologies have emerged that are intended to meet the demands of safety-related ITS. These include the ETSI G5 system and the LTE V2X system. There are significant differences in the way these systems are designed and in the way they are intended to facilitate intra-system sharing. Neither of these systems was designed with a view to easy interoperability with alternative systems. ETSI is, however, currently attempting to resolve this issue. It is expected that ETSI will publish two technical reports on ITS system intra-operability (TR 103 666 and TR 103 667) in late 2019.

CBTC systems are intended to improve efficiency in the running of urban rail systems, typically allowing trains to run at under 90 seconds apart. CBTC systems are a different technology to the systems being proposed for road ITS. The use case scenario is different from the road vehicle, where road vehicles are more densely co-located. CEPT Report 71 recognises the challenges of CBTC sharing with road ITS systems. It suggests that CBTC

operate in the frequency band 5925-5935 MHz. It also suggests that CBTC has some priority over road ITS in the frequency band above 5915 MHz where urban rail CBTC and road ITS are co-located.

The compatibility studies underpinning the CEPT Report 71 can be found in ECC Report 290 - Studies to examine the applicability of ECC Reports 101 and 228 for various ITS technologies under EC Mandate (RSCOM 17-26Rev.3).

The ECC will continue to monitor developments in ETSI, regarding intra-operation of alternative ITS technologies. Taken together, these two CEPT Reports, in response to EC mandates, are intended to set out the spectrum parameters that will enable vehicles to operate more safely and more efficiently. Ultimately, they will facilitate the development of truly intelligent transport systems which will improve the user experience, increase safety and reduce the impact of transport on the environment.

**Robin Donoghue**  
**Frequency Management Expert**  
**European Communications Office**

---

# A to Z of Fraud Types

---

## The A to Z of Telecoms Fraud Techniques involving E.164 numbers

Most telephone and mobile phone users have been victims - or potential victims - of fraud in their lifetime. The tech support scam is one with which many European users will be familiar where a caller pretends to be a computer technician from a well-known company. They say they've found a problem with your computer and ask you to give them remote access to resolve the problem. They then try to make you pay for fixing a problem that never existed in the first place. There is no exact science involved in targeting victims. Scammers make millions of "spam" calls in the hope of finding a victim. This is enabled by developments in technology that allow end users to manipulate CLI and generate multiple spam calls from a single source.

Global spam calls have grown 325% to 85 billion worldwide, according to the first Global Robocall Radar Report, released in February 2019 by Hiya, a Seattle-based company. The report found that Spain, the UK, Italy, France, Argentina and the United States receive the most nuisance and fraudulent calls. Such calls are far and away the biggest consumer complaint to the Federal Communications Commission in the US with over 200,000 complaints each year - around 60 percent of all the complaints it receives.

E.164 telephone numbers often play a role in fraud and misuse. According to the ITU, international E.164 numbering resources are misused when the use 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".

But what are the types of fraud involving E.164 numbers? This article provides an overview of the main types that are commonplace. A combination of the following methods can often be used in tandem to commit fraud.

**CLI Spoofing:** Calling Line Identification (CLI) spoofing is a method whereby a fraudster manipulates the telephone number in the CLI field, leading the person they are calling to think that the call has come from a different location, organisation or person. It is commonplace that a national geographic number or a mobile number that the called person recognises is spoofed. Because the end user trusts the CLI, they are more likely to part with credit card details, bank details or other personal information during the call. Often, the fraudsters originate the calls from developing countries where they are unlikely to be prosecuted or even detected.

**International Revenue Share Fraud (IRSF):** This is one of the oldest and most perpetrated forms of fraud facing the telecoms industry, proliferating particularly with the growth of mobile phones. With IRSF, the fraudsters artificially inflate traffic volumes to certain sections of the national numbering ranges - usually to premium rate numbers. As premium rate numbers are based on a revenue sharing payment model, the end-users of the premium rate numbers receive a payment for each call they receive. Withholding of payments to these end-users is one way of eliminating such fraud.

**Wangiri:** A Japanese word meaning ‘one ring and drop’, Wangiri is a scam whereby the caller cuts off just as the phone rings. The person receiving the call sees a missed call message with an international number displayed as CLI. If they call the number back, usually a premium rate or high tariff destination number, they will be charged a lot of money. Here, the fraudster usually uses an automated technique to simulate multiple calls in a very short period of time. You’ll often see many people within an area receive calls close together and telecoms operators monitor traffic patterns in an attempt to identify wangiri traffic so that the calls can be blocked or the presentation of the CLI for such calls can be restricted quickly.

**Refiling/re-origination of traffic:** Here, the fraudster manipulates the originating number by replacing the “A number” in the call signalling of the real originating country outside the European Economic Area (EEA) with a number from a country within the EEA. They do this because the call termination tariffs differ between EEA and non-EEA countries due to intra-EU roaming regulations. This creates an arbitrage opportunity for bad actors in the value chain and causes problems for both the transit and terminating operators whose revenues are affected. End-users are also affected as they cannot reach the calling party if they try to call back using the CLI presented.

**Hacking of accounts/PBX:** In this case, the fraudster hacks a telephone account or corporate private branch exchange (PBX). They then generate traffic to premium rate numbers as described earlier with IRSF. The victim is then billed for the call origination charges while the receiver of the call on the premium rate number receives a payout from their terminating operator.

**Traffic collectors and roaming fraud:** Using what are known as Subscriber Identity Module (SIM) boxes, the fraudsters generate artificial traffic to premium rate numbers, known as "traffic collectors". The perpetrators often use stolen SIM cards from people who are travelling and roaming in other countries. The home network will eventually block the SIM when the customer reports it stolen but not before the perpetrator has made a large number of calls.

**Malware in apps:** Some unofficial app stores have applications containing malware that can generate calls to premium rate or high tariff numbers. The end-user is often unaware that they have downloaded the malware until their bills come through by which time the

fraudsters have made their money.

**Subscription fraud:** In this case, a fraudster will subscribe to a telecom service but intends on never paying for it. They tend to use false identities and stolen credit card details to set up the subscription. At the other end of this scale, the end-user subscribes unknowingly to a service after clicking on pop-ups on the internet. The subscription charge will appear on their phone bills.

**Call hijacking / short stopping:** When a caller makes a call, the call must flow from the originating operator through one or more transit operators to a terminating operator before reaching the end user. Call hijacking or short stopping occurs when a “dishonest” operator ends the call on their network before it reaches the destination. If a call is intercepted by a transit operator with a recorded announcement, the transit operator can charge the originating operator for the total transit and termination fee. Often, though, only some of the traffic is rerouted to unassigned numbers so few complaints are initiated, making detection less likely.

Telecoms fraud is a high volume, low value business. In cases where potentially thousands of consumers are defrauded of small amounts of money then the chance they will make a complaint is low. Also, as the fraudsters are often located in developing countries, the local authorities do not pursue them as the complaints are made by victims in other countries where the authorities do not have the necessary jurisdiction to take action.

The industry mindset towards combatting fraud has started to shift. Consumer protection now commands a similar priority to revenue protection and collaboration and cooperation between law enforcement authorities, operators and regulators, both nationally and internationally, is increasing. ECC Report 275, prepared by the ECC’s Working Group Numbering and Networks, examines the motives methods and opportunities for committing fraud and makes a number of recommendations for best practices to effectively tackle fraud. The report calls on all stakeholders to share information and collaborate, and as a first step in this direction, WG NaN organised a public workshop on the role of E.164 numbers in international fraud and misuse of electronic communications services in Brussels on 11 December 2018. The next article in this edition of the ECC Newsletter provides a summary from the public workshop. Read it [here](#).

**Freddie McBride**

**Deputy Director**

**European Communications Office**

# Report from Fraud Workshop

---

ECC Working Group Numbering and Networks (WG NaN) provides a platform for stakeholder dialogue on telecoms fraud at its public workshop in Brussels, 11 December 2018

In 2017, the telecommunications industry lost almost US\$30bn to fraud. As enabling technology continues to push intelligence to the edge of the network, the use of electronic communications services to perpetrate fraud is an increasingly difficult challenge for the industry to overcome.

With this in mind, regulators, policy makers and industry gathered in Brussels on 11 December 2018 for a WG NaN Public Workshop entitled "The Role of E.164 Numbers in International Fraud and misuse of Electronic Communications Services".

More than 90 representatives from a broad range of stakeholders came together at the Belgian Institute for Postal Services and Telecommunications (BIPT) to share their experiences and insights on the subject.

## The scale of the problem

Telecoms fraud comes in many shapes and forms and it is a global phenomenon that requires a global response (another article in this edition of the ECC Newsletter provides an A to Z of fraud techniques which you can read [here](#)). The motivation for fraud is often linked to organised crime. All of this activity takes place over a global mesh of interconnected networks where it can be difficult to distinguish between legitimate and illegitimate traffic in an ecosystem that processes billions of transactions and communications sessions each day.

The latest available figures from the Communications Fraud Control Association (CFCA) show that the telecommunications industry lost US\$29.2bn to fraud in 2017. In his keynote address, Jason Lane-Sellers, president of the CFCA and director of solutions consulting at ThreatMetrix, noted that while fraud loss in revenue terms shows a downward trend, fraud attempts are increasing year-on-year. Mr Lane-Sellers also noted that one in 10 online account login attempts is now a fraud attempt which is a sobering thought for consumers and businesses alike.

## What can be done to prevent fraud?

At the workshop, WG NaN Chairman, Johannes Vallesverd, introduced the recently adopted [ECC Report 275](#). The report not only examines the motives, methods and opportunities for committing fraud, but also looks at the administrative and technical tools that are being developed to tackle fraud and misuse.

ECC Report 275 makes a number of recommendations for best practices. These include regulations on CLI spoofing, the need for transparency and raising awareness, encouraging real-time data analytics and promoting information sharing and cooperation. In fact, promotion of information sharing and cooperation was one of the biggest themes to emerge from the workshop, which in itself represented a first step in this direction.

## Collaboration is key

In her presentation, Katia González, head of Fraud Prevention at BICS, said that "trust, partnership and collaboration" are key to combatting international fraud, sentiments that were echoed by other speakers throughout the day. She called for a collaborative approach to ensure international carriers work only with parties who can demonstrate their active commitment to preventing fraud. She also recognised the emergence of a coordinated wholesale carrier approach throughout the industry which in itself is an encouraging development as more and more entities in the value chain make fraud prevention a strategic priority. Ms González also referred to crowdsourcing as one way in which operators can collaborate and be alerted to fraud quickly and to take appropriate action decisively.

Ramona Ciripan of Voxbone said that when an instance of fraud and misuse is detected it can be beneficial to share related information between operators and other relevant stakeholders. This process can be steered by the competent telecommunications authorities. She warned though that the process can only work if confidence and trust is created between the stakeholders and information is shared based on a mutual collaboration.

## The regulator's role

Fraud is a crime and is a matter for law enforcement authorities in the first instance. However, tackling fraud is a major challenge for law enforcement given the global nature of networks and the constraints of jurisdictional boundaries. In these circumstances, telecoms regulators have an important role to play in eliminating the opportunities for fraud through technical and administrative means particularly where E.164 numbers play a role. In his opening remarks at the workshop, Jan Vannieuwenhuyse, BIPT, highlighted the need for a greater focus on fraud by European regulators and, over the course of the day, many speakers called for closer collaboration between industry and regulators as it was considered vital for an effective response. When it comes to numbering, there are certainly administrative and technical means that could be deployed which would have a positive

impact. A key question though is whether regulatory efforts should be focused on supporting law enforcement and the industry or whether regulators should have a leading role? This is an interesting question that was addressed during the panel discussion.

## Regulator-led Initiatives

Tom Boyce, head of the International Unit at ComReg in Ireland, presented on the Body of European Regulators for Electronic Communications' (BEREC) examination of cross-border fraud and its exploration of information sharing methods to tackle fraud. BEREC developed a process for sharing information on potential fraud that would allow European operators to react by blocking traffic or withholding wholesale payments. Mr Boyce pointed out though that the terms "fraud" and "misuse" are often not defined by individual authorities and this can be problematic for operators who need to make decisions fast.

As an active contributor to the International Telecommunications Union's (ITU) work on dealing with fraud and misuse, Dr Richard Hill described the ITU Telecommunications Standardisation Bureau's (TSB) ongoing work to revise ITU-T Recommendations E.156 and E.157. Recommendation E.156 in particular outlines the procedures that the TSB should undertake when it receives reports of alleged misuse from members, including methods to address and counter any alleged misuse.

Both of the above-described information-sharing initiatives may be regarded as being regulator-led where information is gathered and then shared with law enforcement authorities, regulators and operators across the globe. The fundamental issue with this type of approach is the speed with which initial reports are submitted to the ITU or BEREC and the speed with which the information is disseminated and acted upon.

Information needs to be shared in almost real time and from multiple sources in order to generate intelligence which can be used to take decisive action. Sources include information from traffic analysis, crowdsourced information from end-users and information sharing between operators. It is recognised within the industry that many operators fail to remove fraudulent content from their networks because of contractual obligations and the fear of mistakenly blocking legitimate traffic that may look suspicious. Issues surrounding customer privacy and inter-operator contracts remain obstacles to a full-on assault on fraudulent activity and operators need to have confidence in the intelligence they have at their disposal before taking action. Regulatory support would benefit in these circumstances. Multiple sources of information are therefore necessary to ensure that decisions taken to restrict fraudulent activities are based on accurate and reliable intelligence.

On the subject of fraud investigations, Peter Coulter, AT&T, made suggestions for improvements in the way such investigations are conducted in Europe. Mr Coulter pointed out that in the US there is a "regulatory regime which encourages cooperation between

carriers in the traceback and trace forward of fraudulent traffic". Carriers are permitted to share otherwise private information in support of fraud investigations. That framework, which allows cooperative call tracing, supports carriers and regulators alike in the fight against telecoms fraud. Mr Coulter said it could be potentially applied in Europe - an interesting observation given that a new ePrivacy regulation is currently being considered. "Customer privacy must give way to this tool for fraud investigations if we are to be successful in stopping fraudulent exploits involving signalling abuse," he said.

David Maxwell from GSMA, described an initiative by its members to share information with each other on the latest high-risk numbering ranges which are reported by network operators to GSMA. During the presentation, Mr Maxwell called on regulators to introduce stricter controls over the assignment and leasing of national number ranges and by publishing and maintaining up-to-date numbering plans in order to assist the industry in the fight against fraud. Educating consumers to the dangers of fraud and raising awareness is also an important component of reducing fraud. Mr Vannieuwenhuyse pointed to the success of campaigns to raise awareness and educate end-users the banking sector in reducing fraud and protecting consumers.

## Emerging technologies may help

Blockchain technology could help in the fight against nuisance calls and fraud and Elizabeth Greenberg from Ofcom UK provided information on a research project to look at blockchain technology which has been undertaken in the UK. Results from this project are expected sometime later this year or early next year. Another useful development is the SHAKEN/STIR protocols which if implemented could be used to authenticate numbers used as CLI in communications networks. SHAKEN/STIR is now being widely deployed in the US and could reach European shores in the not too distant future.

## Next Steps for WG NaN

The workshop provided a lot of food for thought on what telecoms regulators can do to support the industry and protect consumers. New work items, such as an ECC Report on CLI spoofing, an update of the ECC's guidelines on CLI, and principles for call blocking and withholding payments have been agreed with work on the CLI spoofing already under way.

Further information on the workshop, including the programme and presentations, is available [here](#).

---