CEPT ECC
Electronic Communications Committee

ECC Report 360

Definition of missing, invalid, or fraudulent CLI

approved 28 November 2024

0 EXECUTIVE SUMMARY

Calling Line Identification (CLI) spoofing has been increasing during the last years with a very negative impact not only for end-users but also for operators. ECC Report 338 on CLI spoofing [1] contains in the conclusion, under the form of six points, possible actions for CEPT administrations to take to help mitigate or stop CLI spoofing. The proposed Report implements the conclusions contained in the first and last bullet points of number 2 of the ECC Report 338.

As a conclusion, the three definitions may be summarised as follows:

- Missing CLI is when the CLI or equivalent fields are empty;
- An invalid CLI is a CLI that does not respect the international format as defined in Recommendations ITU-T E.164 [5] ,the rules related to international calling party number delivery in Recommendation E.157 [6] or national rules on the format of the CLI;
- Fraudulent CLI is any CLI that has been used to mislead the recipient and/or the operators by not correctly identifying the caller or is using numbers that are not permitted as CLI by national legislation.

It is considered appropriate that these definitions are used, in a harmonised way among CEPT administrations, to allow procedures not only related to determination of termination rates but also to decide action, such as filtering or blocking calls, in the interconnection between operators.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Abbreviation	Explanation
CEPT	European Conference of Postal and Telecommunications Administrations
ECC	Electronic Communications Committee
CLI	Calling Line Identification
PAI	P-Asserted Identity
PPI	P-Preferred Identity
EU	European Union
EC	European Commission
ETSI	European Telecommunications Standards Institute
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
OI	Originating Identification
OTT	Over-The-Top
PBX or PABX	Private (Automatic) Branch Exchange
SIP	Session Initiation Protocol
SMS	Short Message Service
SS7	Signalling System No. 7

1 INTRODUCTION

CLI spoofing has been increasing during the last years with a very negative impact not only for end-users but also for operators. ECC Report 338 on CLI spoofing [1] contains in the conclusion, under the form of six points, possible actions for CEPT administrations to take to help mitigate or stop CLI spoofing. The proposed Report implements the conclusions contained in the first and last bullet points of number 2 of the ECC Report 338.

There are several places where the terms “missing, invalid or fraudulent” CLI are used, but these terms are not clearly defined. When the CLI is considered as missing, invalid or fraudulent, operators may decide to block the calls, to remove the CLI from any further routing or to change the CLI according to the (inter)national rules and apply higher wholesale interconnection rates. This could have implications on multiple aspects.

For instance, some operators change the CLI in order to mask the origin of the call, in particular changing the CLI for traffic originating from a number from the national numbering plan of a country that does not apply the Delegated Regulation (EU) 2021/654 [2] setting the Eurorates to a CLI from the national numbering plan of a country that is part of the Eurorates zone. The objective is to make the terminating operator believe that the traffic originates from a number pertaining to the national numbering plan of a Eurorates country, in order to take advantage of the cheaper termination fees that apply in the Eurorates zone. In this way, fraudulent income can be generated.

Moreover, the practical application of having a harmonised interpretation of the notions “missing, invalid, or fraudulent CLI” goes beyond the domain of interpreting what operators can do in the context of the Eurorates Delegated Regulation. For instance, having harmonised definitions can contribute more clarity to operators regarding what actions may be taken to combat CLI spoofing and other forms of telecom fraud. For instance, in accordance with ECC Recommendation(23)03 [3], CEPT administrations may mandate that all calls with a CLI that is either invalid or fraudulent could be blocked in order to stop all forms of fraud that relies on invalid or spoofed CLIs.

Therefore, without a common understanding of these terms, disputes may arise between operators on the handling of calls with a CLI that is considered by one of the operators involved in the conveyance of the call as falling within these categories. It is therefore important to establish a common understanding of what qualifies as a missing, invalid or a fraudulent CLI, in order to encourage a common approach.

End-users may also face negative impacts when the CLI is missing, spoofed to show an invalid number (e.g. from an unassigned range) or it fraudulently shows a CLI belonging to another end-user (e.g. a trusted bank). In these scenarios, call-back would be impossible on invalid numbers or when the CLI is missing, and fraudulent use of third parties’ CLI would not identify the real caller and possibly expose the receiving party to fraud.

2 DEFINITIONS

Term	Definition
Eurorates	Single maximum Union-wide mobile voice termination rate and a single maximum Union-wide fixed voice termination rate to be charged by providers of wholesale voice termination services for the provision of mobile and fixed voice termination services.

3 LEGAL BACKGROUND

Fraudulent use of numbers and identifiers in communications not only poses a threat to trust in number-based interpersonal communications services, but also has a potential to reduce the general level of trust between citizens in domestic and international societies, which may in turn result in numerous negative societal consequences.

The overall legal situation in Europe is that there is little or no specific regulation at a European level, and fragmented regulation on the national level. While some countries have established regulatory frameworks and implemented numerous measures to combat fraud, others are still in the early stages of developing their regulatory mechanisms.

The extent of overall European financial loss related to fraud is not clear, although national figures indicate high and increasing financial loss. For instance, in Norway the overall loss was over 86 million EUR in 2023[1], in Latvia 4,5 million EUR in the first four months of 2024[2] and in Sweden the National Fraud Centre of the Swedish Police estimated gains from vishing/smishing related to fraud for 2023 to 60 million EUR [3]. In the United States (of America), the Federal Trade Commission reports that the annual loss was over 10 billion USD in 2023[4].

The *modus operandi* for telecom fraud may vary. Besides techniques intended to incur lower termination tariffs, current telecom fraud methods include Wangiri, PABX-hacking and spoofing (also associated with social engineering) leading up to credit card or account fraud. Fraud is not only conducted through services which make use of legacy technologies but also through Over-The-Top (OTT) services. Furthermore, fraud is not only reliant on spoofed numbers and identifiers, but also through content, e.g. fraudulent link in Short Message Service (SMS) or OTT-messaging.

3.1 CONSIDERATIONS ON THE EURORATES DELEGATED REGULATION

One *modus operandi* for telecom fraud is the "termination rate fraud" in the context of the Eurorates Delegated Regulation, and this will be described in the following two sections.

3.1.1 The regulation is about calls between (E.164) numbers, not countries or networks

Article 1 of the Eurorates Delegated Regulation [2] specifies: "*Articles 4 and 5 shall apply to calls originated from and terminated to Union-numbers*" (Articles 4 & 5 are the articles setting the price caps for mobile and fixed Eurorates respectively). The applicability of the Eurorates does not seem dependent on the actual caller's location but related to the calling and called numbers.

In the EC's staff working paper (explaining how to interpret the Eurorates), the EC gave the following example (attached, page 25, footnote 63):

"*In accordance with the proposed definition of termination services, which is based on the number, it results that, for instance, the roaming calls made by a Belgian number to a Dutch number when the Belgian end-user is travelling in Switzerland will fall within the scope of the Regulation. These calls are originated from a Union-number (the number of the Belgian end-user) and terminated to a Union-number also (the Dutch number).*"

As such, if we follow the same logic of this example, a call from a Swiss tourist (with Swiss number, i.e. not part of the Eurorates zone) in Belgium, making a call to a Dutch number, would not be in scope for the Eurorates.

[1] Norske banker ble svindlet for nesten én milliard i fjor | DN

[2] Latvijas četru lielāko banku klientiem četros mēnešos izkrāpts 7,1 miljons eiro (retv.lv)

[3] Brottsvinster för bedrägerier ökade under 2023 | Polismyndigheten (polisen.se)

[4] https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

3.1.2 Application of the Eurorates Delegated Regulation

In current practice the rate for a call can be determined based on the destination number (B-number) and the originating number (A-number). The origin in this case cannot be based on parameters controlled by the terminating operator and can easily be changed by external parties, e.g. a transit network.

Recital 10 in the Eurorates Delegated Regulation states that the regulated rates for voice termination services should apply to calls originated from and terminated to a number included in national numbering plans corresponding to E.164 [5] country codes for geographic areas belonging to the territory of the Union (Union-numbers).

Terminating providers determine the origin and destination of a call from the originating number and destination number communicated in the call-related information received from preceding operators in the chain of conveyance for that call.

The origin of the calls should be based on the network provided number, not the presentation number provided, e.g. by the originating end-user, as the network provided number identifies the origination of the call.

The route of a call, the networks from where the call enters, has no influence on the termination rate. Defining the origin of the call based on the identification of the route, is, in most of the cases, not possible.

Recital 15 of the Eurorates Delegated Regulation states that: "*As the origin of the call would define whether the Union-wide termination rates apply or not, it is essential for Union operators to be able to identify the country of origin of the caller. For this purpose, operators may rely on the country code within the calling line identification (CLI). In order to ensure a correct application of this Regulation, Union operators should receive a valid CLI assigned to every incoming call. Consequently, Union operators would not be bound to apply Union-wide termination rates to termination of calls if the CLI is missing, invalid or fraudulent.*"

CLI and equivalent fields can be manipulated by parties not under control of the terminating provider. By spoofing / modifying (CLI) parameters in an inter-network signalling, parties can influence the termination rate of a call.

In order to facilitate the implementation of the relevant provision of the Eurorates Delegated Regulation for operators in Europe, a harmonised interpretation of the notions missing, invalid or fraudulent CLI is recommended.

4 MISSING, INVALID OR FRAUDULENT CLI

Signalling System No. 7 (SS7) contains parameters that, for each call, specify whether a calling party number should be presented or restricted to the called party. The number is shown to the called party only if the value is set to presentation allowed. In an outgoing call from a Private Branch Exchange (PBX), if it is allowed and the number is not present, the network provided calling party number will be included in the CLI parameter to be presented to the called party.

However, SS7 is getting more and more obsolete due to the migration to Voice over IP. Equivalent arrangements exist in the Session Initiation Protocol (SIP) which is used for voice over IP with the following fields:

- The “From” header field contains the Originating Identification (OI)/Calling Line Identification (CLI) that the user wants to pass transparently through the network to the destination. This is comparable with a user-provided (i.e. a non-verified generic E.164 number) parameter in Integrated Services Digital Network (ISDN) User Part (ISUP);
- The “P-Asserted-Identity” (PAI) header field is designed to carry the network-provided identifier (in ISUP the corresponding parameter is the Calling-Party-Number parameter coded as network provided). This field should normally only be configurable by the originating service provider, but depending on the implementation, may be configurable also by the user and/or by intermediary service providers and, therefore, is not always reliable;
- The “P-Preferred-Identity” (PPI) header field is designed to give the user the possibility to input user generated information. According to the relevant ETSI standard [4], the value input shall be checked by the network to see if it is one of a stored list of identifiers registered by the subscriber and authorised by the network. If the value is not in this list then it will be replaced by a default identifier;
- The “Privacy” header field gives users the possibility to restrict the presentation of their identifier contained in the P-Asserted-Identity header.

The ECC Report 338 on CLI spoofing also concludes that:

- An explicit prohibition of CLI spoofing, not only for operators but also for users, should be considered in national legislation;
- The further elaboration of harmonised regulatory guidelines and/or mandatory rules in CEPT countries on how to deal with CLI is appropriate and this may include, amongst others:
  - The definition of unambiguous technical rules for determining which traffic qualifies as spoofed;
  - Offering more legal certainty, if needed, for operators that block traffic as a result of suspected CLI spoofing activity;
  - Studying or proposing solutions to address the extent to which 'interconnection surcharges' may be levied by terminating or transit operators, in justified circumstance.

4.1 MISSING CLI

The concept of a missing CLI is when the CLI or equivalent fields (e.g. FROM/PAI fields) are empty.

4.2 INVALID CLI

An invalid CLI is a CLI that does not respect the international format as defined in Recommendation ITU-T E.164 [5], the rules related to international calling party number delivery in Recommendation ITU-T E.157 [6], e.g. the “Country Code” has to be included in the calling party number) or national rules on the format of the CLI (e.g. number length as defined by the Numbering Plan Administrator, e.g. a Belgian mobile number has the following format +32 4PQ AB CD EF).

4.3 FRAUDULENT CLI

A fraudulent CLI is any CLI that has been used to mislead the recipient and/or the operators by not correctly identifying the caller including the use of numbers that are not permitted as CLI by national legislation.

Examples of fraudulent CLIs are:

- Any instance where the CLI has been illegitimately modified (e.g. not according to applicable national legislations) by an operator or illegitimately sent by the originating end-user;
- CLI which corresponds to a number from unallocated numbering ranges in the national numbering plan, or to a number that has not been assigned for use;
- A CLI which corresponds to a number not assigned to an end-user, or is assigned to an end-user but is used, without authorisation, by another end-user;
- CLIs which correspond to numbers (e.g. premium rate numbers) which cannot be used as CLI according to national legislations.

5 CONCLUSIONS

As a conclusion, the three definitions may be summarised as follows:

- Missing CLI is when the CLI or equivalent fields are empty;
- An invalid CLI is a CLI that does not respect the international format as defined in Recommendation ITU-T E.164 [5] ,the rules related to international calling party number delivery in Recommendation ITU-T E.157 [6] or national rules on the format of the CLI;
- Fraudulent CLI is any CLI that has been used to mislead the recipient and/or the operators by not correctly identifying the caller or is using numbers that are not permitted as CLI by national legislation.

It is considered appropriate that these definitions are used, in a harmonised way among CEPT administrations, to allow procedures not only related to determination of termination rates but also to decide action, such as filtering or blocking calls, in the interconnection between operators.

ANNEX 1: LIST OF REFERENCES

[1] ECC Report 338: “CLI spoofing”, approved June 2022

[2] Delegated Regulation (EU) 2021/654 of 18 December 2020 – supplementing Directive (EU) 2018/1972 of the European Parliament and of the Council by setting a single maximum Union-wide mobile voice termination rate and a single maximum Union-wide fixed voice termination rate. Available here

[3] ECC Recommendation (23)03: “Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers”, approved November 2023

[4] ETSI TS 183 007: "Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); Protocol specification". Available here

[5] ITU-T Recommendation E.164: "The international public telecommunication numbering plan". Available here

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