GIRAF global Recommendation 2026 – 01, v.1

on

Possible regulatory measures to combat illegitimate CLI spoofing

As approved by #18 GIRAF 12 May 2026

Introduction

Digitally enabled fraud, which is typically carried over multiple channels and technologies, represents a global societal problem. It causes both substantial financial loss as well as emotional distress to the victims, and it undermines trust in the electronic communications services.

The Global Informal Regulatory Antifraud Forum (GIRAF) asserts that effective and urgent action is required. Competent National Regulatory Authorities ("regulators") must, at minimum, implement decisive measures to incentivize stakeholders to prevent fraudulent traffic.

One particular enabler of fraud is illegitimate manipulation of telephone numbers, also known as CLI spoofing.

In this framework, GIRAF addresses the present Recommendation to the regulators. Its aim is to guide regulators in choosing relevant antifraud measures to protect end users from the ever-increasing, practice of illegitimate CLI spoofing. The recommendations put forward are based on the inputs from participants in GIRAF, a group which provides an informal forum for more than 40 regulators from around the globe.

GIRAF hereby states:

Taking into consideration that:

1. The global rise of fraudulent and spoofed traffic is eroding trust in electronic communications and fuelling illegal digital activity,
2. The Global Anti-Scam Alliance estimates in their Global State of Scams 2025 Report that consumers from 42 countries lost $442 billion to scams in the past year,
3. The challenge of fraud cannot be solved by regulators, operators or carriers alone, Multistakeholder cooperation is a crucial key in the global fight against fraud and illegitimate spoofing,
4. Several regulators have taken measures to prevent illegitimate CLI spoofing and many others are considering taking similar steps. However, most countries have not introduced such measures and people remain vulnerable to illegitimate CLI spoofing,
5. A lack of action to tackle this issue will only serve to encourage and incentivise fraudsters and those who seek to conduct illegitimate CLI spoofing,
6. The origin and impact of illegitimate CLI spoofing can be domestic or international, and consequently international cooperation between regulators and industry is essential to tackling the problem,
7. Regulators around the world may have different approaches to tackling illegitimate CLI spoofing and other forms of digitally enabled fraud, reflecting their national contexts, regulatory frameworks, culture of multistakeholder cooperation, and the structure of their national networks,
8. The development and implementation of best practices to tackle illegitimate CLI spoofing should be swift, clear and realistic,
9. The scope of this Recommendation is limited to illegitimate CLI spoofing on international calls using national CLIs. Additionally, SMS, MMS or RCS and spoofing of international CLIs are excluded from the scope of this Recommendation,

with reference to

10. ITU-T Recommendation ITU-T E.156, Guidelines for ITU-T action on reported misuse of E.164 number resources
11. ITU-T Recommendation ITU-T E.157, International calling party number delivery
12. ITU-T Technical Report TR.spoofing (06/2021) on Countering Spoofing
13. ITU-T Recommendation ITU-T E.371 Deemed impermissible traffic
14. GIRAF Communique nr. 1 on "Carry with Care"

15. ECC Recommendation (23)03 on Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers
16. ECC Report 338 (2022) on CLI Spoofing
17. Europol Position Paper on Caller-ID spoofing, 2025
18. The ongoing multi-stakeholder work in One Consortium and other initiatives
19. UNODC Global Public-Private Partnership Framework against Fraud, from Global Fraud Summit 2026.

recommends

that where applicable to combat illegitimate CLI spoofing regulators could:

1. Shape regulation to reduce the amount of fraudulent traffic originating from, transiting through or terminating in their jurisdiction or national network;

2. Regulate, or in other ways ensure, clear obligations for relevant stakeholders to block traffic or calls in case of illegitimate CLI spoofing. The regulation could include the following measures:

    a. a duty for the operators carrying international traffic to block incoming international voice calls which do not comply with Recommendation ITU-T E.157. Such a duty could also include a requirement to block numbers that are not compliant with national numbering plans;

    b. obligations to establish a DNO (Do Not Originate) register containing e.g. numbers that are only used to receive and not to originate calls. The DNO register may also include unallocated numbers, unassigned numbers and numbers from block and/or allow lists;

    c. operators to ensure compliance with Recommendation ITU-T E.156 (Guidelines for international CLI);

    d. for national geographic/fixed E.164 numbers: to block incoming international voice calls, or at least to suppress/hide the CLI of incoming international voice calls with a national geographic/fixed E.164 number, except in justified cases;

        i. Any exception should be carefully considered and justified, since exceptions may be particularly susceptible to being exploited by fraudsters;

    e. for national mobile E.164 numbers: to block incoming international voice calls, or at least to suppress/hide the CLI of incoming international voice calls with a national mobile E.164 number as CLI where it cannot be confirmed that the subscriber is roaming abroad, except in justified cases. Checks on roaming status, or any other verification, should be carried out while respecting relevant privacy provisions;

        i. Any exception should be carefully considered and justified, since exceptions may be particularly susceptible to being exploited by fraudsters;

    f. operators to use risk-based and adaptive approaches (e.g. calling pattern analysis, behavioural analysis) to identify and mitigate CLI spoofing;

3. regulate, monitor and enforce obligations to mitigate CLI spoofing for international carriers incorporated in, or operating within relevant domestic jurisdiction, hereby ensuring that the obligations also apply to them;

4. monitor and enforce compliance with regulation and consider imposing penalties or other sanctions or consequences in case of non-compliance with regulated obligations to mitigate CLI spoofing;
5. ensure that any measures adopted do not jeopardise the handling of legitimate incoming international voice calls or block nationally permitted exceptions;
6. proactively seek and gather information on ongoing trends and data in fraudulent traffic, to acquire a better understanding of the occurrence of fraudulent traffic;
7. support and engage in national and international multi-stakeholder arenas for cooperation against digital fraud. These arenas may include participation from electronic communications providers, law enforcement agencies, financial institutions, regulatory bodies from other jurisdictions, and relevant national and international authorities. The arenas may include sandbox initiatives experimenting on what data can be shared between sectors, such as for example the banking and telecom sectors, in order to prevent fraud;
8. ensure that relevant privacy considerations are made and that guidance is given to stakeholders in order to reduce risk of non-compliance with privacy rules, to this end, it is advisable that regulators, where applicable, strengthen dialogue with data protection authorities, particularly in the context of combating CLI spoofing;
9. raise awareness with stakeholders that the absence of detailed regulation does not preclude stakeholders from collaborating, experimenting and exploring solutions to combat fraudulent activities;
10. support and/or promote consumer awareness activities to enable the end user to reduce exposure to spoofing related fraud.

***

The recommendations outlined in this document are non-exhaustive and non-mandatory in nature and could be implemented in their entirety as well as selectively, dependent on the regulatory framework of the relevant jurisdiction. The recommendations could be implemented nationally either formally through legal acts or by means of voluntary industry standards, or a combination of means.

These recommendations may be reviewed and/or updated by GIRAF periodically as required by GIRAF participants.

About GIRAF

The Global Informal Regulatory Antifraud Forum (GIRAF) is an informal forum of experts launched in June 2024, with the goal of fostering multilateral collaboration among NRAs, enhancing global cooperation with the international communications industry (e.g. One Consortium), and other key stakeholders.

GIRAF's initial objective is to establish a framework of non-binding, harmonised recommendations, best practices, and guidelines. The initiative is inclusive and free to join, operating on an opt-in basis and open to all NRAs or public competent authorities with similar regulatory responsibilities, allowing participation according to available resources.

GIRAF operates as a neutral, independent, and non-binding initiative led by regulators. While providing a platform for dialogue and cooperation, individual NRAs retain full sovereignty and remain free to determine whether and how to implement GIRAF's guidelines and recommendations.