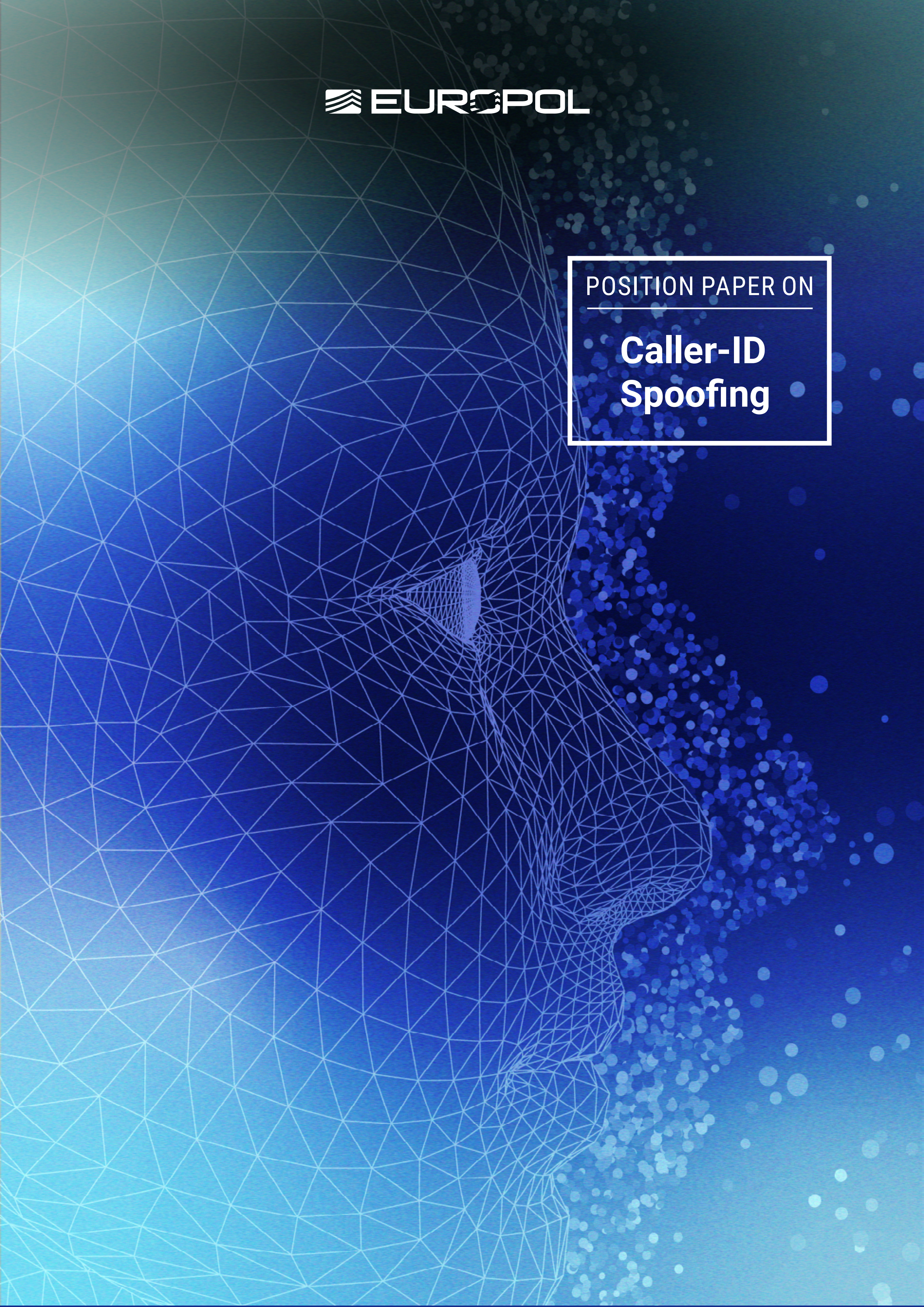
EUROPOL



POSITION PAPER ON

Caller-ID Spoofing

BACKGROUND

Spoofing, specifically caller ID spoofing, drives financial fraud and enables social engineering scams, resulting in substantial economic and societal damage, with an estimated EUR 850 million lost worldwide annually. Phone calls and texts are primary attack vectors, accounting for approximately 64% of reported cases.[1] This is done by deliberately manipulating the information displayed on a user's caller ID, often using Voice over Internet Protocol (VoIP) services or specialised apps, to show a false name or number that appears legitimate and trustworthy. The ability of malicious actors to conceal their true identity and origin, severely impedes the capacity of law enforcement agencies (LEAs) to trace and prosecute cybercriminals.

PURPOSE

This paper aims to highlight the urgent need for a coordinated, multi-faceted approach to mitigate cross-border caller ID spoofing. It outlines the essential technical, regulatory and collaborative measures required to address this critical global issue – protecting citizens and enabling the work of LEAs across Europe.

Example: Poisoned Networks

In July 2021, prior to the launch of Finland's anti-spoofing initiative, Finnish telecommunications operator, Elisa, monitored a dramatic surge in fraudulent calls. Up to 90% of daily incoming calls from abroad, during weekdays, were identified as fraudulent. These attackers predominantly used caller ID spoofing to appear to be calling from local numbers, exploiting user trust. The fraudulent call peaks coincided with typical office hours, indicating a targeted and organised campaign designed to maximise impact during business operations. This illustrates how core communication infrastructure can become 'poisoned' by pervasive, deceptive traffic, posing a severe threat to both network integrity and user safety.

[1] GASA, 2024, Global State of Scams Report, source: https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-ins-12-months-gasa-feedzai.

EU LAW ENFORCEMENT REALITY

LEAs throughout the EU consistently observe diverse modus operandi (MOs) for spoofing attacks across various crime areas, underscoring the pervasive nature of this threat. Criminals frequently spoof caller IDs to impersonate trusted entities like banks, government agencies, utility companies, or even family members, in scam calls for the purposes of committing fraud such as tricking recipients into revealing sensitive information, making fraudulent payments,
or initiating money transfers under false pretences.

Similarly, in tech support scams, spoofing enables scammers to appear as legitimate tech support services, convincing victims of non-existent computer 'problems', leading to demands for payment, malware installation, or remote access for exploitation.

Furthermore, a dangerous form of harassment, known as swatting, involves perpetrators spoofing caller IDs to make it seem as though an emergency call originates from a victim's address, triggering large-scale emergency responses.

Organised criminal networks intentionally operate from different countries when launching caller ID attacks against citizens of other nations. This strategy allows them to evade detection and hinder law enforcement investigations, thereby creating safe havens for their schemes. These networks often establish 'spoofing-as-a-service' platforms to automate caller ID spoofing, with the aim of lowering the barrier for others to be able to commit crimes. By offering such services, criminals can easily impersonate banks, LEAs or other trusted entities.[2]

Position: Europol urges action to rebalance spoofing investigations

From a public safety and operational standpoint, the current situation where spoofing is easy to perpetrate but hard to investigate is untenable. Europol's strategic objective, in line with the EU's internal security strategy, is to support an environment that imposes significant technical costs and complexity on criminals engaged in spoofing. This must be coupled with efforts to streamline regulation and enhance the efficiency of lawful investigative processes to ensure accountability across the Union.

[2] Action against criminal website that offered 'spoofing' services to fraudsters: 142 arrests; Europol, 2022, https://www.europol.europa.eu/media-press/newsroom/news/action-against-criminal-website-offered-%E2%80%98spoofing%E2%80%99-services-to-fraudsters-142-arrests.

CHALLENGES IDENTIFIED BY EUROPOL AND EU MEMBER STATES (MS)

A Europol survey of LEAs conducted across 23 countries revealed significant challenges in implementing anti-caller-ID spoofing measures. This means that the combined population of approximately 400 million people remain susceptible to these types of attacks.

These challenges include:

Limited established contact and collaboration with telecommunication operators.

> There is a need for stronger communication channels and partnership with telecommunication operators, which is crucial for information sharing related to spoofed calls.

Need to broaden engagement with essential stakeholders.

> This highlights the importance of engaging with all relevant parties, including national regulatory agencies (NRA), telecommunication companies and industry experts, who are essential for implementing comprehensive anti-spoofing strategies.

Need for suitable regulatory frameworks or updated legislation.

> This identifies the requirement for more effective regulatory frameworks specifically designed to address caller ID spoofing attacks and enable law enforcement to act decisively.

Need for clearer police mandates and increased resources to initiate solution.

> This points to the requirement for adequate resources and explicit authority for LEAs to be able to effectively combat caller ID spoofing attacks.

Challenges in identifying the problem.

> This points to a need for enhanced understanding of the technical intricacies, scope, and the pervasive impact of caller ID spoofing attacks on investigations across diverse MOs.

Need for improved communication channels with NRAs.

> This shows the importance of better communication with regulatory authorities to facilitate the development and enforcement of effective policies to combat caller ID spoofing.

Challenges in securing full cooperation from telecommunication operators.

> This indicates the need for greater willingness and collaborative efforts from telecommunications companies in implementing and maintaining robust anti-spoofing measures.

STRATEGIC OBJECTIVES

Addressing spoofing requires a strategic approach: balancing technical efficacy, policy adaptation and collaborative action. Key strategic issues and their corresponding solutions are summarised below.

HARMONIZATION OF TECHNICAL STANDARDS

The fragmented technical implementations across nations create vulnerabilities exploited by attackers, and therefore require a unified EU-wide approach.

Objective	Description
Establish robust international traceback mechanisms.	Develop a neutral and cross-jurisdictional system for hop-by-hop tracing, requiring standardised processes for information sharing and robust APIs/signalling checks.[3,4]
Distinguish legitimate from illegitimate spoofing.	Implement mechanisms to validate inbound international calls with national CLIs [5] (e.g. home network verification for roaming).[6] This may include leveraging solutions like API-based caller ID verification [7] as an out-of-band method, or considering in-band solutions which directly inspect and block calls from identified spoofed caller IDs within their network's primary communication path, thus avoiding latency issues.[8]
Leverage and harmonise existing industry tools.	Survey, categorise and promote a vendor-neutral 'toolbox' of solutions (e.g. Do Not Call (DNC)/ Do Not Originate (DNO lists, unallocated number lists, blacklisting, malformed number detection) with standardised interfaces.

CROSS-BORDER COLLABORATION

The transnational nature of spoofing attacks demands seamless information sharing and coordinated action among Internet Service Providers (ISPs), telecommunications providers, law enforcement and regulatory bodies.

Objective	Description
Foster European regulatory and industry collaboration.	Enhance fight against fraud by creating a unified, coordinated ecosystem for information sharing and enforcement, reducing reliance on lengthy mutual legal assistance processes. Build on and enhance legal access mechanisms like the EIO[9] to further facilitate evidence sharing among EU MS. Support initiatives that bring together industry and regulators to co-develop global guidance and best practices.

[3] One Consortium, 2024

[4] Traficom, 2022, Recommendation to Telecommunications Operators on Detecting and Preventing Caller ID Spoofing.

[5] CLI stands for Calling Line Identification and refers to the telephone number of the calling party that is transmitted through the telecommunications network and displayed on the recipient's phone or caller ID device.

[6] Traficom, 2022, Recommendation to Telecommunications Operators on Detecting and Preventing Caller ID Spoofing.

[7] GSMA, 2024, Call Check, source: https://www.gsma.com/solutions-and-impact/industry-services/call-check/

[8] Elisa, 2025, Call Fraud Prevention Solution, source: https://elisa.com/carrierservices/operator-solutions-and-services/fraud-call-prevention-solution/.

[9] EIO is a legal instrument established under EU law (Directive 2014/41/EU) that aims to streamline and speed up cross-border evidence collection in criminal investigations between EU MS.

REGULATORY CONVERGENCE

Differences in national regulations impede effective cross-border investigations and criminal prosecution. Harmonising legal frameworks and enforcement mechanisms is essential to achieving a unified and effective European response.

Objective	Description
Policy Implications for Traceback.	Establish harmonised national legal and regulatory frameworks for legitimate traceback requests, including clear rules on who can issue such a request, what can be shared and with whom, alongside enforcement agreements.
Policy implications for legitimate/illegitimate spoofing.	Provide regulatory clarity on acceptable spoofing use cases and mandate service providers to implement validation mechanisms, defining responsibilities for blocking illegitimate traffic, such as reverse onus clauses (burden of proof).
Policy implications for industry tools.	Encourage regulatory bodies to mandate or incentivise the adoption of proven tools and foster ongoing collaboration between industry and regulators to adapt to evolving fraud techniques.
Policy implications for global collaboration.	Drive harmonisation of regulatory approaches and promote international cooperation among telecommunications authorities, recognising the need for multi-stakeholder engagement. This includes evaluating the suitability of diverse authentication frameworks, thus recognising that a one-size-fits-all approach (like STIR/SHAKEN)[10] may be at odds with national laws or EU-privacy norms.

Example: Finnish anti-spoofing initiative

The Finnish approach highlights the need for multi-stakeholder engagement across the private and public sector (PPP). It outlines a technical approach that primarily involves blocking international calls operating under a Finnish number unless their legitimacy can be verified. This verification of Finnish calls from abroad is achieved through two conceptual methods: direct inter-operator validation, where receiving operators query number portability and perform location checks with the subscriber's home network; or via a proxy server model, in which validation requests are centralised. If validation fails, indicating a spoofed or unverified number, the call is not connected to the subscriber; instead, it is either released or redirected to an indication device that plays a ringtone.

[10] FCC: https://www.fcc.gov/call-authentication; accessed: July 2025.

CONSIDERATIONS BEYOND CALLER-ID SPOOFING MITIGATION

While robust anti-spoofing measures are crucial, and have proven to reduce fraudulent caller ID spoofing traffic in core networks, it is imperative to acknowledge and prepare for new and evolving trends in online crime that will continue to pose significant challenges.

These threats include already existing SIM-based scams that leverage fake or stolen identities, indicating a need for enhanced identity verification processes in the telecommunications industry (KYC).[11]

Anti-regulatory subleasing, where telecommunication resources are exploited outside regulatory frameworks, will require vigilant monitoring and stricter enforcement (KYT).[12] The existence of anonymous prepaid services also presents a persistent challenge for tracing illicit activities.

Furthermore, 'callback scams' such as those observed in the case of Microsoft call support scams, where victims are lured into returning calls to fraudulent lines, highlight the continued ingenuity of criminals to bypass newly introduced limitation and adapt new MOs.[13]

Lastly, the broad and ever-evolving landscape of SMS and numerous smishing (SMS phishing) variants will require continuous adaptation of detection and prevention strategies, even as direct caller ID spoofing is being tackled.

QUO VADIS?

In order to effectively combat caller ID spoofing, Europol calls for harmonised technical standards for traceback and spoofing detection, enhanced cross-border collaboration among LEAs, regulators and industry, and aligned regulatory frameworks in order to facilitate legitimate traceback requests and anti-spoofing measures.

These efforts directly align with the key objectives of the ProtectEU strategy , safeguarding societies and democracies from online and offline threats and enhancing the EU's capacity to combat organised crime. Furthermore, recognising that caller ID spoofing is a primary enabler of online fraud, these measures contribute to the commitment under the ProtectEU strategy for combatting this serious crime through strengthened prevention, more effective law enforcement action and victim protection.[14]

Through multi-stakeholder collaboration, to address emerging threats and develop effective countermeasures, digital security can be significantly enhanced. This will ensure citizens are better protected from the adverse effects of caller ID spoofing.

[11] KYC: 'Know Your Customer' is a process for businesses, to verify the identity of their clients and assess their suitability and potential risks before or during the course of a business relationship.

[12] KYT: 'Know Your Transaction' for mobile operators, extends beyond just financial services to encompass the monitoring and analysis of various activities occurring over their network to detect and prevent fraud, abuse, and illicit activities.

[13] MO: a "modus operandi" is a characteristic method or procedure, especially one used by a criminal or an attacker, to carry out their actions.

[14] ProtectEU: A European Internal Security Strategy, European Commission, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0148.

POSITION PAPER ON CALLER-ID SPOOFING

PDF | ISBN: 978-92-9414-055-5 | doi: 10.2813/4992564 | QL-01-25-017-EN-N

Neither the European Union Agency for Law Enforcement Cooperation nor any person acting on behalf of the agency is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2025

While best efforts have been made to trace and acknowledge all copyright holders, Europol would like to apologise should there have been any errors or omissions. Please do contact us if you possess any further information relating to the images published or their rights holder.

Cite this publication: Europol (2025), Position Paper on Caller-ID Spoofing, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu