White Paper

HardenStance

Proven Ways to Block Caller ID Spoofing Scams

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

ENEA

February 2025

Executive Summary

- Phone calls are the most common media used for online scams. Using caller ID spoofing with scams can be very effective at gaining a victim's trust and persuading them to empty out their own bank account. For that reason, telcos are more likely to consider volumes of these calls to be "high" than any other type of voice fraud.
- Now that pioneer countries have shown how voice firewalls can be used for effective blocking of caller ID spoofing, telcos in other markets need to do the same. International regulatory alignment is needed but it shouldn't be an excuse for delay.
- Querying outbound mobile roaming traffic is the sweet spot in a layered approach to blocking malicious caller ID spoofing. Solutions must align with local competences, privacy and security rules, and emerging global industry guidelines.

Download the accompanying Briefing: "Enea's Voice Firewall for Telcos"

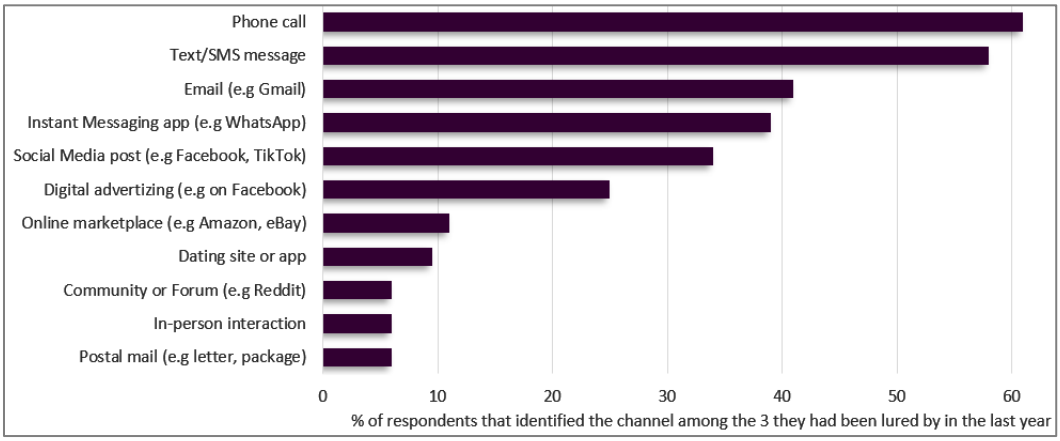
Caller ID spoofing originated with the rise of VOIP software. To this day, tweaking the PBX files can make an outgoing phone call display any caller ID of choice.

An incredibly easy way to win a victim's trust

Caller ID spoofing originated with the rise of VOIP software being used to convert analogue phone calls to a digital signal and route them via a PBX. To this day, tweaking the PBX files can make an outgoing phone call display any caller ID of choice. There are legitimate use cases for CLI spoofing. It allows businesses to make reminder calls that customers will recognize as worth answering, not ignoring. Some remote workers need to display their company's main number when they're using their laptop to make business calls from home. But because VOIP software is openly available, it has also been used to commit fraud over many years. If PBX files are amended to show the caller ID of a local police department or the tax office, or someone's bank, a quick online search will often confirm to the called party that that number is indeed associated with the local police department, tax office or their bank. Historically, people have had no need to know that these numbers are typically only used for incoming not outgoing calls.

We tend to have high trust in the integrity of telecom services. That trust is compounded by the trust we also tend to have in the authority of the police, tax department, our banks and other institutions. It renders most of us predisposed to trust the 'help' provided by those we believe to be their representatives. That predisposition to trust is accentuated by the very convincing way scammers communicate with their victims. They are often meticulously prepared. They may already have an initial subset of personal information on a target before they even make first contact. They wield that information during the scam so as to deepen the target's trust. With that, they can create a convincing sense of fear and urgency for us to act in what they tell us is our own best interests. **Figure 1** shows how online scammers use phone calls more than any other media. In most countries, a sizable share of the calls represented use CLI spoofing.

Figure 1: Phone calls are the single most common media used for scams



Source: The Global Anti Scam Alliance: "The Global State of Scams 2023"

Figure 2: Actual cases of scams that use caller ID spoofing to defraud victims

Date reported	Victim (country)	Scammer's techniques, including caller ID spoofing	Amount lost
2022	Milly Clark (UK)	(i) Smishing text requesting update of account details. (ii) Later, HSBC bank's phone number spoofed in call advising urgent transfer of funds to avoid fraud.	£22,000
2022	Dr Patricia Harney (U.S)	(i) Bank's phone number spoofed on call advising unusual activity, so a new card needed issuing. Details shared.	$3,500
2022	Alan Rickitt (UK)	(i) Text advising Barclay's Bank fraud department will call (ii) Barclays phone number spoofed in call to advise of fraudulent activity.	£49,500
2024	Several (Minnesota, U.S.)	(i) Sheriff's office phone number spoofed to demand payment of fines for having missed jury duty or risk jail. (ii) Directed to make payment, in some cases by inputting $100 bills into a supermarket-hosted cash-collecting machine linked to a crypto-currency account.	$4,000 in one case
2024	Anonymous (Nevada, U.S)	(i) Bank's phone number spoofed in a call to warn of suspicious account activity. (ii) "Courier" urgently despatched to victim's home. Victim's card taken and cut in two but ensuring chip was undamaged.	$9,000

Source: HardenStance/media reports

Figure 2 highlights a number of high profile cases reported in the media around the world of how scammers have used Caller ID spoofing as a key component in scams, whereby the victim is tricked into directly or indirectly participating in the transfer of funds out of their own account to the scammer.

The large amounts of money defrauded from the victims reflect the high level of trust that the spoofed caller ID helps inspire. The level of access to their sensitive information the victim is willing to share can allow scammers to potentially drain a victim's bank account of all its funds rather than merely abuse a credit card, for example.

Scammers increasingly pursue targets across multiple platforms

Increasingly, scammers pursue their targets across different platforms. As well as via telephony, they track them and interact with them across SMS and email, and newer messaging apps like WhatsApp and collaboration platforms like Teams. They also augment scams with AI to deepen trust still further. They have started using Generative AI to compose more convincing phishing emails or smishing texts and to augment caller ID spoofing with identity spoofing using fake audio and video representations of people that are known to the victim. The combination of a legitimate looking caller ID and a recognizable-sounding voice on the other end of the phone can bypass the defences of even the most wary and untrusting of individuals.

For the victims of these types of scams, the experience is intensely personal. From a broader societal perspective, however, it tends to be sharp spikes in the total numbers of victims and the aggregate scale of impacts that trigger government and industry to act to better protect citizens. And the aggregate numbers have become alarming and unsustainable in recent years.

Here are a few examples of the impact of CLI spoofing in different countries:

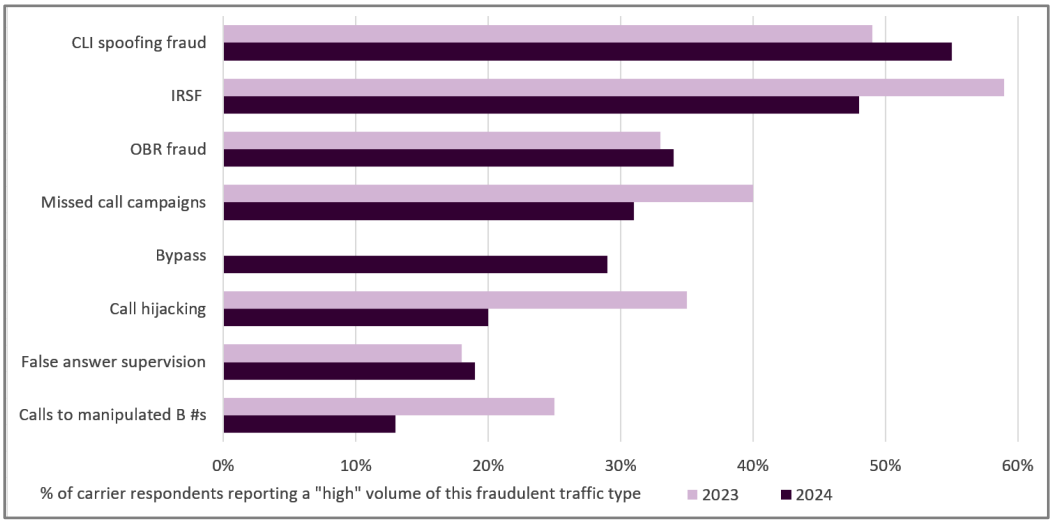
- **Australia: losses to bank impersonation scams averaged $22,000**. In 2022, Scamwatch, run by the Australian Competition and Consumer Commission (ACCC), received 14,603 reports about bank impersonation scams, many of which leveraged Caller ID spoofing. Losses averaged $22,000 and more than 90 reports were recorded of losses between $40,000 and $800,000.
- **Finland: €7.1 million lost to technical support scam calls alone**. Traficom, the Finish regulator, reported that in 2020 and 2021 Finnish people lost approximately €7.1 million to technical support scam calls alone.
- **UK: 170,000 victims of just one caller ID spoofing service**. When the UK's National Crime Agency (NCA) reported the arrest of the administrators of the "Russian Coms" caller ID spoofing service in August 2024, it shared some data about the group's activities. The NCA estimated losses to victims in the "tens of millions" of pounds, including 170,000 victims in the UK alone. Russian Coms placed 1.3 million calls to 500,000 unique phone numbers in 107 countries. 170,000 of these calls lasted longer than 5 minutes, which implies a successful fraud.
- **Turkey: 60 victims per day reporting voice fraud to the Chief Public Prosecutors Office**. In 2022, the Istanbul Chief Public Prosecutor's Office set up a special department with 3 dedicated prosecutors to investigate an average of 60 reports of phone scams per day. One victim reported a loss of ₺500,000 ($36,690).

In the 2024 Global Leader's Forum survey, telco respondents were more likely to consider CLI spoofing to be "high" than any other category of voice fraud.

Caller ID Spoofing is only one among many types of voice fraud

Telcos have a great many types of voice and messaging fraud to contend with. Some defraud the telco itself while others – like Caller ID spoofing – scam the end user. The telecom sector as a whole doesn't have a very good record when it comes to preventing, detecting and mitigating fraud. Too often it turns a blind eye and accepts losses. That said, it's clear from the 2024 Global Leader's Forum (GLF) survey of telco survey takers depicted in **Figure 3** that CLI spoofing fraud has shot up the priority list. Asked how they viewed recent volumes of several different types of voice fraud, telco respondents were more likely to consider CLI spoofing to be "high" than any other category.

Figure 3: Of all types of fraud, CLI spoofing is most likely to be viewed as "high"



Source: International Telecoms Week's Global Leader's Forum (GLF) Survey 2024

Industry's response – past, present and future

The vulnerability of telecom services to malicious caller ID spoofing as well as other types of fraud and security risk has been known about for many years. SS7 is a very old signaling protocol. It was designed without any embedded security features, back in the days when government-owned monopoly telcos only exposed their signaling to one another as trusted partners - not to multiple third parties as is common now.

Until recently, telcos were largely left to themselves to determine whether or not a solution to the problem of CLI spoofing was needed – and what any solution might look like. But as the volume of malicious spoofed calls - and the severity of the impact on victims - has grown in recent years, regulators, banks, and law enforcement have become increasingly motivated to act. The four phases of industry's response to the risk from CLI spoofing poses are depicted in **Figure 4** and described below.

Starting in around the 2020 timeframe some countries began responding to increased volumes of scams using CLI spoofing and increasingly severe impacts on citizens.

Phase 1: Pervasive fatalism

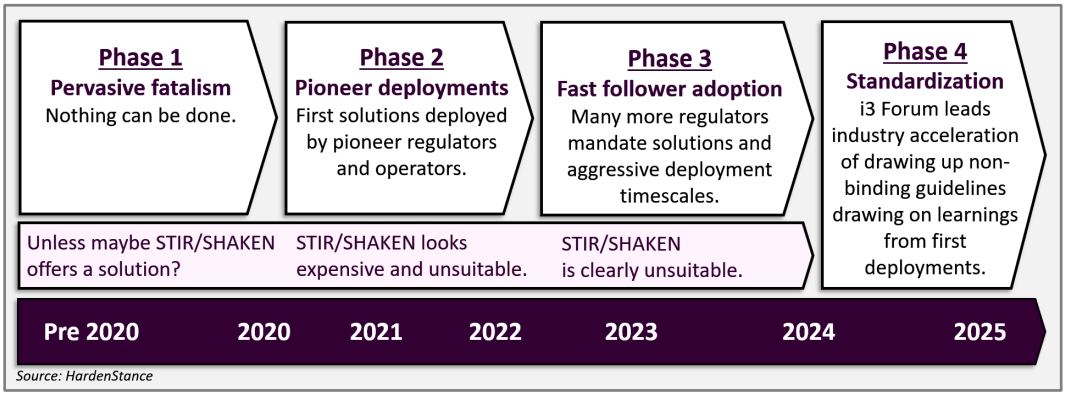
Before 2020, telcos tended to be both negligent and fatalistic about malicious CLI spoofing. Instances of abuse tended to be fairly low, and their impacts were relatively small. Telcos themselves were only indirectly impacted and not very much at that. There was little motivation to act. In any case there was no readily available fix.

The only global standard potentially capable of addressing the problem at that time was the U.S STIR/SHAKEN standard. Although approaches in France, Brazil and India still appear to be at least partially leveraging elements of STIR/SHAKEN, that global vision has not taken off. The general consensus now is that STIR/SHAKEN is unlikely to see much adoption for CLI spoofing outside North America, and especially not in Europe. Much of the rest of the world has concluded that effective caller ID blocking can be delivered faster, at significantly lower cost, and with greater certainty than by using STIR/SHAKEN. The near-universal worldwide adoption that it would need to render STIR/SHAKEN effective at blocking caller ID spoofing isn't going to materialize.

Phase 2: The can-do pioneers of 2020 - 2023

As shown in **Figure 4**, starting in around 2020 a few countries such as Australia, the UK, Finland and Egypt began responding to increased volumes of scams using CLI spoofing and/or increasingly severe impacts on citizens. In these countries, pioneer operators acting independently or coordinating with their national regulator designed and deployed their own pre-standard blocking solutions. These are among the countries that kick-started a much more constructive, can-do, Phase 2 response from industry. As described in **Figure 5**, these fixes have achieved very significant results in terms of blocking a high share of the CLI spoofing calls in markets where they have been deployed. The banks, regulators and law enforcement authorities were important to driving this second phase by engaging far more purposefully with the telecom sector.

Figure 4: The 4 phases of industry's response to CLI spoofing



Source: HardenStance

Phase 3: The fast followers of 2024

Starting from the end of 2022, the achievements that pioneer countries were able to point to triggered a sharp rise in the number of regulators and operators working to get solutions implemented in their own markets. This Phase 3 response from fast followers got underway in 2023 but began scaling up sharply during 2024. As shown in **Figure 5**, Ireland, Sweden, Belgium and India are among these fast followers.

Phase 4: The drive for standardization in 2025

The last year or two has seen leading regulators demanding more from industry in terms of coordinating common guidelines for addressing the problem. Starting with the Conference of European Post and Telecommunications administrations (CEPT) publication of ECC Recommendation 23 (03) on "measures to handle incoming international voice calls with suspected spoofed national E.164 numbers" in November 2023, Phase 4 is now well underway. Drawing on the learnings from the initial implementations of Phase 2 pioneers, Phase 4 is seeing industry put energy and urgency into creating global standards for blocking malicious CLI spoofing.

Figure 5: Caller ID spoofing blocking initiatives by Phase 2 'Pioneers' and Phase 3 'Fast Followers'

Date	Country	Organization	Type of organization	Achievement/Target
Phase 2 – The Pioneers of 2020 - 2023				
December 2020	Australia	ACMA	Regulator	Telcos mandated to block scam calls. As of Q1 2024, Australian telcos had reported blocking 1.9 billion scam calls to ACMA.
July 2022	Finland	Traficom	Regulator	Blocking measures mandated. By November 2023, Traficom stated that scam calls from spoofed Finnish numbers had "finally come to an end in practice."
August 2022	UK	EE	Operator	Stated it is blocking up to 1 million scam calls every day that use CLI spoofing.
June 2024	Egypt	Telecom Egypt	Operator	Effective blocking measures resulted in a 90% reduction in spoofed calls.
June 2024	Latvia	Bite	Operator	70,000 spoofed international calls blocked in the first two weeks since block went live.
Phase 3 – The Fast Followers of 2024				
April 2024	Ireland	Comreg	Regulator	Final Decision following consultation mandates that telcos must block fixed and mobile CLI spoofing within six months.
May 2024	India	Ministry of Comms	Regulator	India's telcos mandated to implement a solution co-designed with the Ministry to block incoming international spoofed calls.
June 2024	Belgium	Parliament	Legislature	Telcos given 3 months to block calls spoofing Belgian landlines, 6 months to block calls spoofing mobiles.
October 2024	Sweden	PTS	Regulator	Telcos must remove fake CLIs or block in the case of international fixed calls by November 2024 and international mobile calls by March 2025.

Following initial work by bodies like CEPT and the GSMA's Fraud and Security Group (FASG), the i3Forum launched its 'Restore Trust in International Telecommunications' initiative of March 2024. This now has 34 leading telecom operator and vendor members as well as participation at various levels by other industry bodies such as GSMA, the Alliance for Telecommunications Industry Solutions (ATIS); the Cloud Communications Alliance (CCA); the Communications Fraud Control Association (CFCA): the U.S Industry Traceback Group (ITG): the Global Leaders Forum (GLF); and the Global Solutions Council (GSC).

Two sub-groups have been created by the i3Forum:

- **The One Consortium**. This had 40 telco members as of October 2024. Working Groups are due to publish their first reports during Q1 2025.
- **The Global Informal Regulatory Antifraud Forum (GIRAF)**. This comprised 29 National Regulatory Authorities (NRAs) at the end of October 2024, of which 24 were European. Its mission is stated as "to produce non-binding harmonized (where possible) recommended best practices and guidelines – for the industry and for NRAs."

The objective of forming these two separate groups is so that they can develop their positions as discrete groups with distinct interests and then negotiate and resolve differences as coherent blocks rather than in a less structured way.

There isn't any one single measure that will block 100% of these calls. Rather the cumulative effect of multiple measures can drive a high rate of effective blocking in excess of 90%.

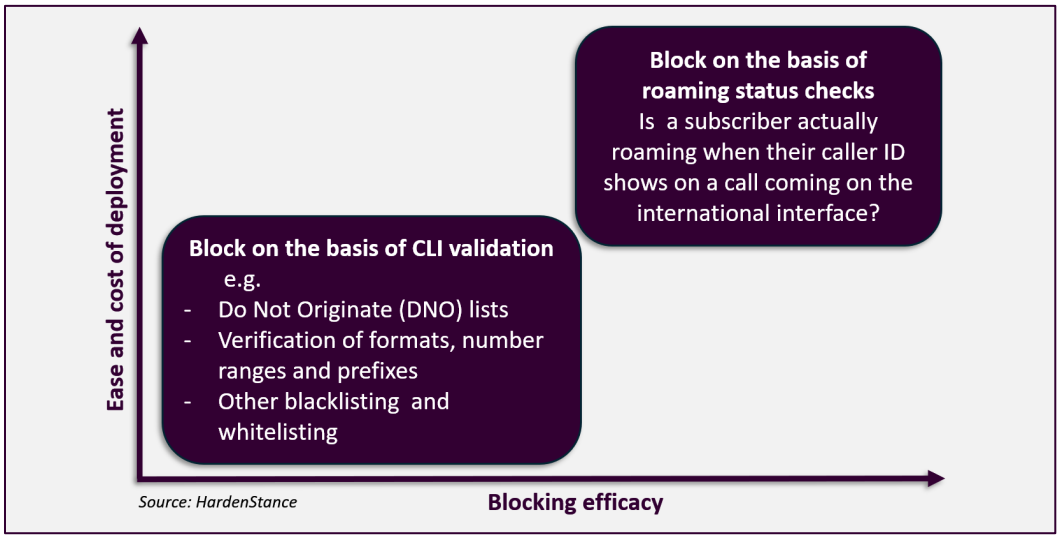
The likely shape of industry guidelines to come

The loss of support for the STIR/SHAKEN standard demonstrated clearly that it isn't a silver bullet. Moreover, the experience of pioneers and fast followers is that there is no silver bullet of any kind for blocking malicious caller ID spoofing. There isn't any one single measure that will block 100% of these calls. As depicted in **Figure 6**, the experience in pioneer markets is that multiple layers are needed; it's the cumulative effect of multiple layers that can drive a high rate of effective blocking in excess of 90%.

Do No Originate (DNO) lists

The low hanging fruit among options available to telcos and regulators is Do Not Originate (DNO) lists. As the name suggests these are phone numbers that are known to be used only for receiving calls – they literally 'do not originate' any voice calls. Hence if a DNO-listed number ever presents as an incoming call, it is by definition maliciously spoofed and should be blocked. Examples include the numbers of local police departments, tax offices, tech support desks and banks that only receive incoming calls.

Figure 6: A layered approach to blocking malicious CLI spoofing in the network



Other basic verifications

Telcos can also "allow" or "block" calls according to a number of basic criteria that can be identified and implemented fairly straightforwardly and at low cost. Examples include:

- Blocking a given international number if it does not conform to designated formats, number ranges and prefixes.
- Blocking any national landline numbers coming in via the international interface.

The detection efficacy of all these approaches varies and is heavily dependent on the quality of the data so accessing up to date, accurate, data is key.

Mobile roaming traffic is the sweet spot for blocking CLI spoofing

In most markets, international mobile roaming traffic is the sweet spot for blocking the largest volume of malicious CLI spoofing calls. There are two reasons for this:

- **Mobile calls account for at least 80% of all voice traffic now**. As an example, Ofcom data shows that back in 2022, 84% (170 billion) of the total 202 billion outgoing UK phone calls were made from mobile phones compared with just 16% (32 billion) from landlines.

It's typically through a focus on monitoring incoming international calls that telcos and regulators can have the single biggest impact on blocking CLI spoofing.

- **A large majority of unwanted and fraudulent phone calls, including malicious CLI spoofed calls, typically originate from overseas.** They mostly originate from call centres operated by gangs in developing countries targeting wealthier individuals in more developed countries. For example, when Elisa, the Finnish operator, embarked on monitoring its international incoming calls in 2021, it found that 90% of all incoming calls joining its network from abroad were displaying a spoofed caller ID which it presumed to be fraudulent.

  In recent years a very high percentage of fraudulent calls have originated in the Indian city of Kolkota, considered to be one of the "scam capitals of the world". Excellent cooperation by law enforcement agencies across national boundaries led to some high profile arrests of Kolkota gang members on their call centre premises at the end of 2024. Such wins by law enforcement are one more important part of a layered approach to combating voice fraud. However, as demonstrated many times over the years, the limitation of these actions is that closing down a big criminal operation can also open up a gap in the market that is then filled by another gang in another city or country.

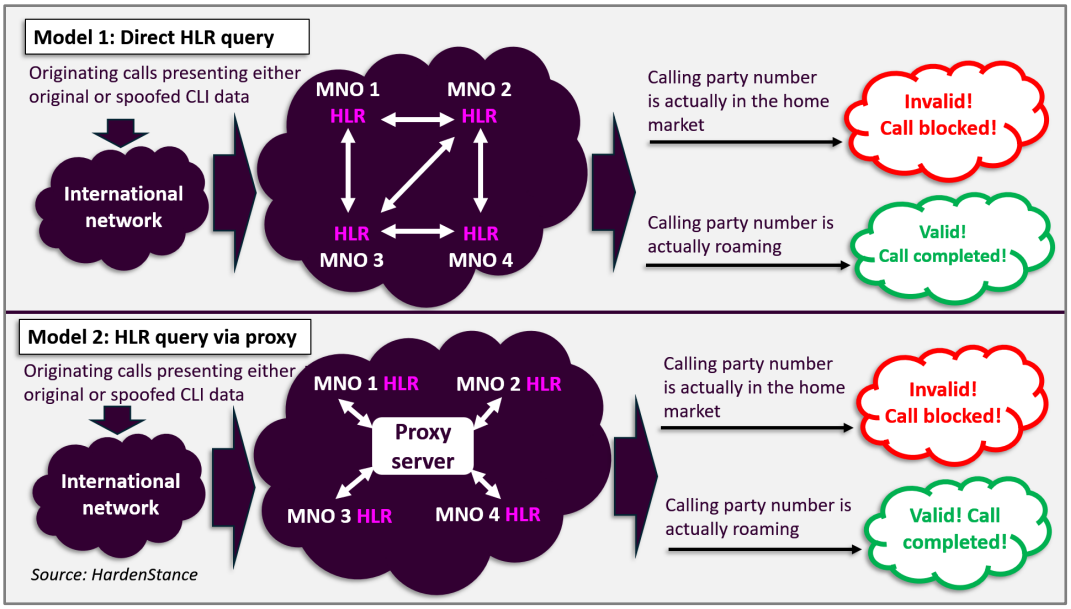
Verification of the status of outbound roamers is the first priority

From a commercial perspective, there's a hierarchy in terms of the types of roaming calls that any one telco or any one national regulator is most motivated to protect against malicious CLI spoofing. Let's consider this mainly from the perspective of a hypothetical Mobile Operator A, as well as from the perspectives of a Mobile Operator B (a domestic mobile competitor) and a Mobile Operator C (a mobile operator in a foreign country).

From Operator A's perspective, protecting its own outbound roamers is its first priority. Its own outbound roamers are vulnerable to highly targeted attacks (e.g spoofing their caller ID for a scam call placed to their spouse). In addition, spoofing that outbound roamer's caller ID could just as easily result in another of Operator A's own customers being scammed or one of Operator B's customers being scammed. The customers of Operator A and Operator B both benefit a lot from Operator A implementing CLI spoofing protection (and vice versa). This should also motivate national regulators to coordinate an industry-wide response around a unified solution architecture.

While still important, the fate of inbound roamers – the customers of Operator C - is a lesser priority for Operator A. To Operator A, Operator C's roamers appear as inbound roamers but they are also Operator C's own outbound roamers. As such, responsibility for protecting these and other users in Operator C's home market falls mainly to Operator C.

Figure 7: Verification options for outbound roamers



Fragmentation in approaches between regions and countries is unhelpful to everyone. A collaborative approach also yields the best outcome at the national level.

To verify that caller IDs that imply they are one of another domestic operator's mobile subscribers while roaming are actually roaming, early adopters have used a number of different approaches. As depicted in **Figure 7**, they have used variants of two main models - direct HLR querying and HLR querying via proxy.

1 **Direct HLR querying:** with a Direct HLR query model, mobile operators have to expose signalling interfaces to one another and send each other details about the status of one another's mobile customers on request and in real time.

2 **Inter-operator HLR querying via proxy.** The alternative to rival operators querying one another's HLRs directly is to deploy a proxy server between them. This allows each operator to provide as well as access the same type of information about one another's customers, albeit in a more anonymized, less intrusive way. In this model, the operator that submits a query to the proxy doesn't know which of its competitors the subscriber is served by. Similarly, the queried operator doesn't need to know from which of its competitors the query is coming from. Usually, the neutral third party best suited to managing a proxy is the national regulator.

Either of the two models has to be executed in a way that protects against compromise of sensitive subscriber information like the user's IMSI, cell ID or Visited Location Register (VLR). A telco's own confidential business information also has to be protected. For that reason some early implementations of the direct query model rely on a bare-bones binary response to a query that either means 'yes' the subscriber is roaming or 'no' they're not. Providing richer context can be helpful for more granular detection but it also carries greater risk of exposing confidential information.

Factors that determine which of the two models is adopted in a given market include the regulator's preference and assessment of the market's ability to execute (and they may not necessarily point to the same answer); the way local or regional privacy laws are implemented and interpreted; and the competitive dynamic between network operators as well as MVNO service operators in the local market.

General guidelines for all ecosystem stakeholders

The experience of lead markets as described in this paper, together with ongoing assessment of the nature of the risk, points to the following guidelines for all stakeholders that are engaged in designing and implementing solutions to block malicious caller ID spoofing:

- **Act – there is no good reason to delay**. As shown in **Figure 5** there are multiple examples of countries and operators that have already delivered very valuable outcomes for their customers by deploying pre-standard blocking solutions.
- **Collaborate proactively in international fora and anchor the architecture and policies in the experience of pioneer countries.** Recognize that using different terminology for describing the same or similar approaches is confusing and drives everyone's costs up. Recognize that fragmentation of approaches across different countries and regions is also unhelpful to everyone.
- **Recognize that a collaborative, multi-party, approach among operators also yields the best outcomes at the national level**. Recognize too that the regulator is inevitably best placed to coordinate the formulation of the right solution architecture and oversee its implementation. If needed, and if it possesses the necessary competence, the regulator may also be best placed to manage aspects of day-to-day operations too.
- **Ensure alignment with local privacy and security rules as well as local competences.** Alignment with emerging global guidelines is important but they are being designed with a view to providing an agreed framework of options that allow for variations in implementations.
- **Balance the speed of deployment with standards-alignment**. Select an architecture that can be implemented quickly – within 6 to 12 months. But ensure that whatever approach is chosen is also able to evolve elegantly in the direction of alignment with global industry guidelines.
- **Recognize that different types of controls are appropriate for different types of telco.** Depending on their business models, it can make sense for one operator but not another to trust a given interconnection partner; or for one but not another to trust high volumes of traffic from a given country. A telco that only connects to other domestic carriers doesn't need to be burdened with implementing the same checks as operators that receive a lot of international traffic.
- **Do not assume that law enforcement will be unsupportive**. The greater scale and severity of impacts of scams enabled by caller ID spoofing often makes law enforcement more willing to commit resources than for other types of voice fraud that are considered to be merely nuisance calls.
- **Plan for future threat intelligence-led phases in voice fraud mitigation.** Historical precedent shows that scammers don't stand still. As soon as one technique is rendered ineffective, they adjust their tactics and try something else. A national framework for blocking malicious caller ID spoofing therefore needs to enable telcos and regulators to keep up with the threat landscape. It needs to be purposely designed to enable it to adapt quickly and effectively - not just to new malicious CLI spoofing techniques but to new types of voice fraud as they arise. Together with learning and information sharing in international fora, this allows stakeholders to be proactive in blocking new types of voice fraud.

A national framework for blocking malicious caller ID spoofing needs to be purposely designed to enable it to evolve to address adjacent types of fraud as they arise

Additional guidance for telecom operators

- **Choose the right person to represent the company in multi-party negotiations with the regulator and with other stakeholder partners.** The individual should have extensive industry experience in their local market. They should also have a high level of authority within their organization so as to command management's attention and communicate the company's position clearly within a collaborative industry forum.

Regulators are tending to mandate implementation of a solution according to aggressive timescales nowadays.

- **Stay ahead of the regulator.** As shown by the Swedish, Belgian and Irish examples in **Figure 5,** regulators are tending to mandate implementation of a solution according to aggressive timescales nowadays. To comply with those timescales, telcos should be implementing and testing solution components in step with phases of the consultation. They shouldn't wait for the consultation to conclude and a solution to be mandated.
- **Institutionalize continuous investment in fraud prevention capabilities.** This should embrace both skills training and development among employees as well as in the latest monitoring, detection and monitoring capabilities, including those that are AI-driven.

Additional guidance for regulators

- **Invest in maintaining up to date data and in automating information sharing.** Ensure data like Do Not Originate (DNO) and other lists are kept up to date. Such data is also still only made available as Excel spreadsheets in most cases, including in many advanced countries. Telcos need to be able to consume this information via an API and feed it directly into their data systems. ■

More Information

- HardenStance Briefing: Enea's Voice Firewall for Telcos
- International Telecoms Week's 'Global Leader's Forum' Survey 2024
- CEPT's ECC Recommendation 23 (03) (November 2023)
- I3Forum Webinar: "One Consortium, GIRAF - One year in, the Restore Trust Initiative is in full swing!" (September 2024)
- Enea Webinar: "Rising above the noise: Managing the barrage of voice fraud" (2024)

About Enea

Enea is a world-leading specialist in software for telecom and cybersecurity. Our cloud-native solutions connect, optimize, and secure services for mobile subscribers, enterprises, and the Internet of Things. More than 90 leading mobile operators deploy Enea in their networks, supporting more than 30% of the world's mobile subscribers.

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cybersecurity research, and a leading publisher of cybersecurity reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cybersecurity. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, OASIS, The Cyber Threat Alliance, MEF, The GSMA, CTIA and ETSI. To learn more visit www.hardenstance.com Register for HardenStance's 2025 "Telecom Threat Intelligence Summit"

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report. HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same. The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.