ENACT.

European Network Against Crime and Terrorism

Annex to Methods to Facilitate the Traceback and Mitigate the Spoofing of Telecommunications

Report Type	Advanced Report
Lead Author	Eric Priezkalns
Dissemination Level	PUBLIC
Date	04/08/2026

Project Information

Grant Agreement Number	101121152
Acronym	ENACT
Name	European Network Against Crime and Terrorism
Call Topic	HORIZON-CL3-2022-SSRI-01-02 Knowledge Networks for Security Research & Innovation
Action Type	Coordination and Support Action
Start Date	01/09/2023
Duration	36 Months
Coordinator	PJ

Document Information

Report Type	Advanced Report
Report Title	Methods to Facilitate the Traceback and Mitigate the Spoofing of Telecommunications
Date	21/08/2026
Dissemination Level	PUBLIC
Main Author(s)	Eric Priezkalns
Contributors	James Greenley

Revision History

Version	Date	Author	Comments
0.1	21/08/2026	Eric Priezkalns	First Draft

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Copyright

Transparency and Disclaimer Statement

This statement is provided for transparency purposes**, highlighting possible conflict of interests**. The author has, in the course of his professional activities, worked with a range of organisations active in the telecommunications and fraud prevention sectors, including some stakeholders and solution providers referenced in this report.

The report was prepared independently and the assessments presented reflect the author's professional analysis of the available evidence and information collected during the study. **The author remains fully responsible for any of the content provided in the report. Results presented in the report do not reflect ENACT's opinions and should not be interpreted as an endorsement of any solution.**

Stakeholders interested in deploying any of the solutions mentioned in the report must still consider all ethical, legal, societal or any other rules and recommendations applicable.

1 Annexes

Annex A: Spoofing and Traceback Survey Questionnaire and Responses

This annex reproduces the questionnaire and the responses received. Respondent wording is reproduced as submitted. Responses from organisations are ordered alphabetically by organisation name; responses from people answering for themselves are ordered by surname.

A.1 Questionnaire

About You

Your name

Are you answering this survey on behalf of an organisation or as a private individual?

Response options:

- On behalf of an organisation
- As a private individual

Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?

Response options:

- I consent to my name being included in the report of the survey findings.
- I want my name to be omitted from the report of the survey findings.

About Your Organisation

These questions were shown to respondents answering on behalf of an organisation.

The name and address of the organisation

A brief description of the organisation's purpose

URL of the organisation's home page

About You as a Private Individual

These questions were shown to respondents answering as a private individual.

Are you resident in a European Union country?

Response options:

- Yes
- No

In which countries or territories do you have relevant experience of spoofing or traceback?

Response options: countries and territories. The full country/territory list is not reproduced in this annex.

Areas of Contribution

Do you wish to contribute your insights about:

Response options:

- 1. Methods to prevent the spoofing of the origin of voice calls
- 2. Methods to prevent the spoofing of the origin of text messages
- 3. Methods to trace electronic communications to their origin

Methods to Prevent the Spoofing of the Origin of Voice Calls

Do you recommend a particular method to prevent the spoofing of the origin of voice calls?

Explain the advantages of the method.

Describe any disadvantages with using the method.

Who owns the intellectual property rights to the method?

Provide any other insights into the methods that can be used to prevent the spoofing of the origin of voice calls that you consider relevant.

Methods to Prevent the Spoofing of the Origin of Text Messages

Do you recommend a particular method to prevent the spoofing of the origin of text messages?

Explain the advantages of the method.

Describe any disadvantages with using the method.

Who owns the intellectual property rights to the method?

Provide any other insights into the methods that can be used to prevent the spoofing of the origin of text messages that you consider relevant.

Methods to Trace Electronic Communications to Their Origin

Do you recommend a particular method (or methods) to trace the origin of electronic communications?

Which kinds of electronic communication can be traced using the method(s)?

Response options:

- A2P SMS text message
- iMessage text message
- P2P SMS text message
- RCS text message
- Voice call to a telephone number
- WhatsApp text message
- WhatsApp voice call
- Other over-the-top (OTT) communications
- Other (free-text response)

Explain the advantages of the method(s).

Describe any disadvantages with using the method(s).

Who owns the intellectual property rights to the method(s)?

Provide any other insights into the methods that can be used to trace the origin of electronic communications that you consider relevant.

Follow-up Contact Details

These optional fields were collected only for to permit follow-up questions to be asked where needed. Respondents' answers to these fields have not been reproduced below.

Email address

Telephone number, including country code

A.2 Survey Responses

A.2.1 Respondents

- 1Route
- A1 Telekom Austria AG
- BTS
- Cleartech S.A
- Doctor Mahshid Delavar
- The Fraud Victim Rights Organization
- Professor Feng Hao
- Heksagon
- jtendo
- Magrathea Telecommunications Ltd
- NeoSoft AG
- NG-BLU Networks
- NICC Standards Limited
- Oculeus GmbH
- Teleindustrien - Telecom Industry Association Denmark
- USTelecom Industry Traceback Group

A.2.2 Responses

A.2.2.1 1Route

About You	
Your name	Jeffrey V. Ross
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About Your Organisation	
The name and address of the organisation	1Route, 386 Howard Clemmons, Granbury, TX 76048, USA
A brief description of the organisation's purpose	Real-time anti-fraud detection/blocking, compliant routing, digital assurance, and location based services.
URL of the organisation's home page	www.1routegroup.com
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls, 2. Methods to prevent the spoofing of the origin of text messages
Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	1Route's On-SIM Digital ID helps prevent voice-call origin spoofing by binding a subscriber's unique identifiers into an encrypted identity that is difficult to clone or falsify. During call setup, the On-SIM solution and 1Route backend can validate the displayed caller ID against trusted identities, blacklist and policy data, and associated fraud signals; suspicious or mismatched calls can be flagged, warned against, or blocked in real time. This adds subscriber-level protection against impersonation, SIM-swap-enabled fraud, and CLI spoofing, especially when combined with 1Route's

	network-level validation and compliant-routing capabilities. For international voice traffic, 1Route combines validation with compliant routing. It verifies the originating number, applies the appropriate standards/regulations/grading and destination-country format, and delivers the call with authenticated caller identity information. This closes the gap where spoofed calls enter through international gateways outside a domestic trust environment (i.e. STIR SHAKEN, MAN, CHAKEN, etc.).
Explain the advantages of the method.	1Route's On-SIM Digital ID provides a lightweight, real-time defense against voice-call impersonation by using an encrypted, multi-factor binding of the subscriber's unique identifiers to detect anomalies that a caller-ID check alone may miss. It can validate incoming caller IDs against trusted and blacklisted identities, identify risks associated with SIM swaps, cloned devices, or account takeover, and warn or block suspicious calls during setup. Because the On-SIM solution operates directly on physical SIMs and eSIMs across 2G–5G networks, it can protect both feature-phone and smartphone users with minimal core-network integration, while supporting stronger customer trust, reduced fraud losses, and fast OTA deployment for operators. Prevents simple CLI spoofing, stops impersonation earlier, creates evidence for decisions, and improves protection against cross-border abuse. Operationally, it works with a layered defense model, supports IP and legacy environments, and avoids unnecessary network replacements. For international traffic, there is no single globally universal voice-authentication standard. STIR/SHAKEN is centered on North American IP networks, while markets can use national CLI validation rules, number registries, country-specific systems such as MAN or CHAKEN, or differing blocking mandates. This creates a fragmented compliance environment for wholesale carriers handling traffic across multiple destinations. This is where 1Route's compliant routing allows the

	different standards to communicate to each other without requiring network changes.
Describe any disadvantages with using the method.	The principal drawback is the On-SIM solution verifies the identity, not whether the caller is honest. It is an important anti-spoofing control, but it does not independently prove the true network origin of every external call across global carrier networks that are not enrolled in the On-SIM solution. The method is best positioned as the identity-trust layer of a broader voice-security architecture—not as a standalone “scam-proof” mechanism. Pair it with real-time behavioral analytics, reputation and blacklist data, fraud rules, and carefully tiered actions such as allow, label, challenge, monitor, or block. 1Route’s positioning reflects this layered approach by combining On-SIM solutions and compliant routing with real-time fraud detection, blocking, analytics, and support for both IP and SS7/TDM environments.
Who owns the intellectual property rights to the method?	1Route / GBSD Technologies
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of voice calls that you consider relevant.	Preventing voice-origin spoofing is most effective as a layered trust-and-enforcement system, not as one protocol. Important methods beyond "signing" a call or number ownership and right-to-use checks, international gateway screening, and mixed-network protection. Merely signing a call is not enough. Validating the authority to use the calling identity, preserving or re-establishing trust across IP and legacy networks, and applying each destination's rules (standards/regulations) to the call due to a single global method not being adopted and network changes are not required globally.
Methods to Prevent the Spoofing of the Origin of Text Messages	
Do you recommend a particular method to prevent the spoofing of the origin of text messages?	A digital ID plus carrier SMS firewall model, supported by a verified business messaging channel for high-risk communications. Unlike voice, there is no broadly deployed validation standard for SMS, so the most practical control is to verify who is authorized to use an alphanumeric sender ID or originating number and enforce that authorization at the carrier edge.

	The approach addresses the core SMS weakness: the sender field is often not inherently trustworthy. A digital ID coupled with terminating-network enforcement makes brand impersonation more difficult because a fraudster cannot simply submit an SMS with a familiar alphanumeric header through any route.
Explain the advantages of the method.	1Route protects SMS origin through a layered Digital Identity Assurance model. It validates digital IDs and originating routes against approved brand and operator records, detects impersonation and look-alikes, enforces decisions through network and SIM-level controls, and delivers genuine communications through verified branded channels. Suspicious messages can be blocked, labeled, or followed immediately with a trusted warning through SMS, USSD, RCS, OTT messaging, push notification, or IVR. 1Route verifies the sender identity, authorized route, and message risk before delivery. The 1Route On-SIM solution adds subscriber-side validation and real-time warnings, while our Messaging Orchestration Platform provides verified branded communication and captures user reports to continuously improve network-wide detection. The business outcome is broader than stopping fake headers: it reduces smishing and OTP theft, helps prevent mobile-money social engineering, protects A2P revenues from bypass, improves customer trust in official messages, and creates auditable evidence for operators and regulators.
Describe any disadvantages with using the method.	Digital-ID is not globally uniform. Controls vary by country, and protection is only as strong as the coverage of local operators, aggregators, registries, and international routes. Some markets have active sender-ID registration programs, while others depend on carrier or aggregator-managed allow lists. Also, an authentic digital ID does not prove that a message or intentions of the sender are safe. Therefore, combine origin validation with account security, traffic baselines, anomaly detection, URL scanning, customer education, and step-up authentication for consequential actions.

Who owns the intellectual property rights to the method?	1Route / GBSD Technologies
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of text messages that you consider relevant.	The most important additional insight is that SMS-origin spoofing is primarily an ecosystem and route-control problem, not merely a content-filtering problem. The most durable defense validates sender ownership, forces delivery through authorized routes, and blocks impersonation at the terminating operator before the message reaches the handset. Make SMS a "notification" channel. Do not let the apparent origin of a text message become the sole basis for a high-risk action. For mobile money, banking, account recovery, SIM changes, and credential changes: Bind confirmation to an authenticated device, SIM-based digital ID, passkey, or risk-based approval process. Apply a cooling off period and additional verification after SIM swap, device change, password reset, or newly added payee events.

A.2.2.2 A1 Telekom Austria AG

About You	
Your name	Petr Kubat
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About Your Organisation	
The name and address of the organisation	A1 Telekom Austria AG, Lassallestraße 9, 1020 Vienna, Austria
A brief description of the organisation's purpose	A1 Telekom Austria AG is a leading telecommunications provider offering mobile, fixed-line, internet, data communication, and digital services for consumers, businesses, and public sector customers in Austria
URL of the organisation's home page	https://www.a1.net/
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls, 2. Methods to prevent the spoofing of the origin of text messages, 3. Methods to trace electronic communications to their origin
Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	Yes. We use an in-house testing system for A-number verification. Our approach is based on active testing. We perform test calls through different international and domestic operators and verify whether the originating A-number is correctly preserved and validated throughout the call path.The testing enables us to identify operators routing with spoofing. Based on the results of our testing, we contact the affected MNOs, inform them about our findings, and discuss possible corrective action - means offer direct

	interconnections to reduce reliance on transit carriers that may enable spoofing and to improve traffic security and transparency.
Explain the advantages of the method.	he advantage of this approach is that it identifies caller ID spoofing through controlled test calls and enables direct cooperation with affected MNOs to address vulnerabilities and improve routing security.
Describe any disadvantages with using the method.	The method is based on controlled test calls and therefore does not provide visibility into all live traffic.
Who owns the intellectual property rights to the method?	A1
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of voice calls that you consider relevant.	No response provided.
Methods to Prevent the Spoofing of the Origin of Text Messages	
Do you recommend a particular method to prevent the spoofing of the origin of text messages?	Austria is currently implementing Sender ID whitelisting for A2P SMS. Only SMS messages using registered and approved Sender IDs are accepted. Messages sent with unregistered Sender IDs, or with variations of registered Sender IDs are blocked. This helps prevent sender ID spoofing, brand impersonation, and smishing attacks.
Explain the advantages of the method.	Only authorized Sender IDs can be used, significantly reducing spoofing and protecting customers from fraudulent SMS messages.
Describe any disadvantages with using the method.	The solution requires registration and maintenance of Sender IDs and effective implementation across the industry.
Who owns the intellectual property rights to the method?	whitelisting database owned by regulator (RTR)
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of text messages that you consider relevant.	The effectiveness of the solution depends on broad adoption by operators, messaging providers, and enterprises

Methods to Trace Electronic Communications to Their Origin	
Do you recommend a particular method (or methods) to trace the origin of electronic communications?	No response provided.
Which kinds of electronic communication can be traced using the method(s)?	No response provided.
Explain the advantages of the method(s).	No response provided.
Describe any disadvantages with using the method(s).	No response provided.
Who owns the intellectual property rights to the method(s)?	No response provided.
Provide any other insights into the methods that can be used to trace the origin of electronic communications that you consider relevant.	No response provided.

A.2.2.3 BTS

About You	
Your name	Sara Ballarín
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About Your Organisation	
The name and address of the organisation	BTS, -- c/ Josefa Amar y Borbón, 10, 500001, Zaragoza (Spain)
A brief description of the organisation's purpose	BTS is a global communications technology company enabling enterprises, operators, and digital platforms to connect, communicate, and innovate through carrier-grade voice, messaging, CPaaS, AI, and Network API solutions.
URL of the organisation's home page	https://bts.io/
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls
Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	Branded calling, number verification, sim-swap detection are some of the methods that could be used to prevent spoofing.
Explain the advantages of the method.	These methods help authenticate the origin and use of the call, as well as the real user making the call.
Describe any disadvantages with using the method.	Implementation is complex and market adoption is not guaranteed as not every carrier may support this authentication technology.
Who owns the intellectual property rights to the method?	n/a

Provide any other insights into the methods that can be used to prevent the spoofing of the origin of voice calls that you consider relevant.	n/a

A.2.2.4 Cleartech S.A

About You	
Your name	Ronaldo Barrozo
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About Your Organisation	
The name and address of the organisation	Cleartech S.A Al. Rio Negro, 585, 12a, Alphaville, Barueri,SP, Brasil, CEP 06454000
A brief description of the organisation's purpose	Cleartech S.A is a Brazilian technology company specializing in mission-critical solutions for the telecommunications industry. With over 25 years of experience, Cleartech S.A provides solutions for systems integration, data processing, number portability, data enrichment, and interconnection revenue assurance, including the control and reconciliation of traffic and financial settlements between operators. In 2023, Cleartech S.A was selected to supply and operate the centralized platform for call authentication and identification (STIR/SHAKEN/RCD) used in the Brazilian market, and has played a leading technical role in the implementation of the Origem Verificada initiative together with Anatel, the Autoridade de Identificação e Autenticação (AIA), and the participating telecommunications operators.
URL of the organisation's home page	www.cleartech.com.br
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls, 2. Methods to prevent the spoofing of the origin of text messages

Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	We recommend the use of STIR/SHAKEN-based caller identity authentication, combined with network-level traffic analysis and fraud and automated-call (robocall) mitigation controls. In general terms, STIR/SHAKEN provides a cryptographic mechanism to authenticate the caller identity carried in the call signaling. The originating network's Authentication Service generates a digitally signed PASSporT (Personal Assertion Token) containing information derived from the call, including the originating telephone number and destination information. This authentication information can then be validated by a Verification Service at the terminating network. In this way, the receiving network can verify whether the caller identity has been authenticated and whether the relevant signaling information has been altered during the process. The underlying STIR architecture is defined by the IETF in RFC 8224, which specifies the SIP Identity mechanism and the roles of the Authentication Service and Verification Service. PASSporT is specified in RFC 8225, while STIR/SHAKEN-specific extensions and the SHAKEN framework are defined through IETF and ATIS standards. The SHAKEN framework also establishes the governance and certificate-management infrastructure required to create a trust relationship among participating service providers. ATIS-1000074 defines the SHAKEN framework, while ATIS-1000080 establishes the governance and certificate-management requirements. In Brazil, this approach is particularly relevant because Origem Verificada, developed with the participation of Anatel and telecommunications service providers, uses STIR/SHAKEN/RCD to authenticate and identify calls. According to Anatel, authentication corresponds to the technical validation of the originating number, while identification enables the presentation of information such as the company name, logo, and purpose of the call.

	The Brazilian architecture also includes the Autoridade de Identificação e Autenticação (AIA), which is responsible for managing the technical ecosystem, including certificates, registration, security policies, and governance. From the fraud-prevention perspective, however, STIR/SHAKEN should not be considered a standalone fraud-prevention solution. Caller-ID authentication increases confidence in the presented telephone identity but, by itself, does not determine whether a call is legitimate or fraudulent. For this reason, we recommend combining authentication with additional controls, such as: • traffic and behavioral analytics; • detection of abnormal calling patterns and high-volume activity; • analysis of robocalls and short-duration calls; • monitoring of changes in calling behavior; • reputation and historical risk information; • rules and/or machine-learning models to assign a risk score to the call; and • blocking, filtering, or applying additional verification mechanisms at the terminating network, based on the identified risk level. This layered approach is important because a fraudster may use a legitimately authenticated telephone number or compromise a legitimate calling environment. Therefore, authentication is primarily effective in addressing caller-identity spoofing, while behavioral analytics and fraud-detection mechanisms address a broader question: whether the call itself can be trusted. In Brazil, Anatel presents Origem Verificada as part of a broader set of measures aimed at combating unwanted and fraudulent calls, rather than as a single solution for all types of voice fraud. This approach is reinforced by binding regulation in Brazil. Resolução Anatel nº 777/2025, of 28 April 2025 (which approved the Regulamento Geral de Serviços de

	Telecomunicações – RGST), together with Acórdão n° 201/2025 (approved in August 2025), made call authentication mandatory on a progressive basis: the initial phase applies to high-volume originators (more than 500,000 calls/month) from November 2025, while full nationwide implementation — covering all originators, including individuals identified by CPF — is required within three years, i.e., by 2028. Public reporting on Origem Verificada (Anatel/operators, March 2026) indicates that approximately 35 billion calls were authenticated during 2025 alone, with 17 mobile operators and 322 fixed-line operators already connected to the platform, illustrating meaningful real-world adoption of the approach we recommend.
Explain the advantages of the method.	The main advantage of STIR/SHAKEN is that it enables cryptographic authentication of the caller's identity, allowing the terminating network — and, where the device supports it, the end user — to distinguish calls whose originating number has been verified from calls whose signaling could not be authenticated. Rather than preventing a call from being placed, authentication substantially reduces the effectiveness of illegal caller-ID spoofing, because a manipulated or unassigned number can no longer be presented as if it were authentic. It increases trust in voice communications and gives operators a standardized, verifiable basis for assessing whether the displayed calling number is legitimate. Real-world adoption in Brazil illustrates the effect at scale: according to public Origem Verificada reporting (Anatel/operators, March 2026), approximately 35 billion calls were authenticated in 2025 alone. The method also improves fraud detection and traceability, helps protect consumers from fraudulent calls, and provides operators with a standardized framework for identifying and managing suspicious traffic.
Describe any disadvantages with using the method.	The main challenges are the complexity of implementation and the need for broad adoption across operators and networks to achieve its full effectiveness. It also requires integration with existing telecommunications infrastructure, ongoing certificate

	management, and proper handling of calls originating from networks that do not support the method. In practice, this complexity is visible in the phased nature of Brazil's own rollout: mandatory authentication currently applies only to high-volume originators, with full coverage of all callers — including individuals — targeted for 2028, and the information actually displayed to the end user still depends on the terminating device and network generation: legacy 2G/3G networks can typically show only the caller's name via CNAM together with a verification mark, while 4G VoLTE/5G VoNR/VoWiFi networks and a compatible handset are needed to deliver the full Rich Call Data (name, logo, and reason for the call).
Who owns the intellectual property rights to the method?	The STIR/SHAKEN protocol is an open standard and is not owned by Empresa X. Cleartech S.A owns its own proprietary platform and technology developed for the implementation and operation of STIR/SHAKEN solutions.
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of voice calls that you consider relevant.	The use of machine learning and deep learning techniques to analyze traffic behavior based on CDRs (Call Detail Records) can provide an additional layer of protection against voice call spoofing and fraud. By identifying anomalous traffic patterns and behavioral deviations, these technologies can help detect and prevent fraudulent activity in real time. Cleartech S.A applies this approach in its own voice-fraud-control platform, which performs real-time analysis of SIP signaling using machine-learning models to detect patterns associated with traffic pumping, unauthorized use of SIP credentials (service theft), robocalls, and Wangiri (one-ring) fraud, and can trigger automated mitigation actions such as call blocking, call diversion, or a CAPTCHA-based challenge, complemented by operator-level, subscriber-level, and global black/white lists.
Methods to Prevent the Spoofing of the Origin of Text Messages	
Do you recommend a particular method to prevent the spoofing of the origin of text messages?	We recommend a multi-layered approach combining SMS firewalling, sender identity validation, and traffic behavior analysis to prevent the spoofing of SMS originators.

	At the network level, an SMS Firewall can inspect signaling and SMS traffic to identify and block messages with unauthorized or suspicious originating addresses. The solution can validate the sender identity against authorized sender information and apply rules based on traffic characteristics, origin, destination, volume, and routing information. Additionally, machine learning and behavioral analysis can be used to identify anomalous traffic patterns and detect fraudulent or spoofed SMS campaigns. Analysis of signaling information and SMS traffic records can help identify deviations from normal behavior and enable real-time blocking or investigation. For messaging security, industry standards such as 3GPP TS 23.040 (Technical realization of the Short Message Service) (https://www.3gpp.org/dynareport/23040.htm) and 3GPP TS 29.002 (Mobile Application Part – MAP) (https://www.3gpp.org/dynareport/29002.htm) define the underlying signaling and service-realization framework within which these controls operate; they do not themselves specify sender-authentication or anti-spoofing mechanisms, which are implemented at the firewall/application layer described above. For IP-based messaging environments, SMPP (Short Message Peer-to-Peer Protocol) (maintained by the SMS Forum, https://smpp.org/) can also be used to control and authenticate connections between messaging platforms and SMS service providers. This approach is particularly effective when combined with operator-level controls, centralized monitoring, and continuous analysis of SMS traffic, providing both preventive controls and the ability to detect new fraud patterns.
Explain the advantages of the method.	The main advantage of this approach is that it provides multiple layers of protection against SMS origin spoofing. It can validate sender identities, detect unauthorized traffic, and block fraudulent messages before they reach subscribers. The combination of rule-based controls and machine learning enables the solution to identify both known and emerging fraud patterns. It also provides greater visibility and traceability of SMS traffic, helping

	operators reduce fraud, protect subscribers, and improve the reliability and trustworthiness of SMS communications.
Describe any disadvantages with using the method.	The main disadvantages are the complexity of integrating the solution with existing operator networks and the need for continuous monitoring and maintenance of detection rules and machine learning models. There is also a risk of false positives, where legitimate messages may be incorrectly identified as fraudulent. In addition, effective protection requires cooperation across operators and messaging providers, particularly for international and inter-network SMS traffic.
Who owns the intellectual property rights to the method?	The underlying signaling and messaging standards referenced above — 3GPP TS 23.040, 3GPP TS 29.002, and SMPP — are industry standards/specifications and are not owned by Cleartech S.A. Any SMS firewall, sender-validation, or machine-learning-based traffic-analysis technology supplied by Cleartech S.A. to implement this approach is proprietary technology developed and owned by Cleartech S.A. or, where applicable, licensed from or provided by its technology partners.
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of text messages that you consider relevant.	An effective approach is to combine SMS firewalling with real-time traffic analysis and machine learning. Analyzing signaling information, sender behavior, traffic patterns, and historical CDRs can help identify anomalies associated with spoofing and SMS fraud. Another important measure is to maintain trusted sender registries and apply appropriate controls to SMS aggregators and inter-operator connections. This enables operators to verify whether a sender is authorized to use a particular originating identity and to block or investigate unauthorized traffic. The use of centralized monitoring and correlation across multiple traffic sources can further improve detection, particularly for large-scale or coordinated fraud campaigns.

A.2.2.5 Doctor Mahshid Delavar

About You	
Your name	Dr Mahshid Delavar
Are you answering this survey on behalf of an organisation or as a private individual?	As a private individual
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About You as a Private Individual	
Are you resident in a European Union country?	Yes
In which countries or territories do you have relevant experience of spoofing or traceback?	United Kingdom
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls
Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	Yes. I recommend Caller ID Verification (CIV), an automated callback method that verifies whether the calling party controls the telephone number displayed on the call recipient's device. CIV applies the familiar security advice of ending a suspicious call and calling the displayed number back, but automates the process so that verification can take place during call setup without requiring action by the recipient. When an incoming call claims to originate from a particular telephone number, the recipient's network temporarily holds the call and places a quickly terminated verification call—similar to a "flash call"—to that displayed number. The verification call carries a randomly generated challenge. The system associated with the genuine number must receive the challenge

	and return the correct response through the original call. A simplified CIV transaction works as follows: - The caller initiates a call and indicates that CIV is supported. - The terminating network holds the original call before ringing the recipient's device. - The terminating network makes an automated, quickly terminated callback to the number that would otherwise be displayed to the recipient. - The callback conveys a short random challenge. The current proposal uses four random decimal digits embedded in the calling number of the verification call. - The originating system receives the challenge and returns the same digits over the original call using Dual-Tone Multi-Frequency signalling. - The terminating system compares the response with the challenge. If they match, the displayed number is marked as verified and the recipient's device is allowed to ring. If the response is missing or incorrect, the call can be blocked, sent to voicemail or delivered with an explicit warning that its caller ID could not be verified. In a SIP implementation, the current proposal introduces: - a civ option tag in the SIP Supported header, indicating that the originating system supports CIV; - a civ-veri-call value for the Purpose parameter of the SIP Call-Info header, identifying the callback as a verification transaction; - the standard SIP Session-ID header to associate the verification call with the original call; - DTMF to return the challenge response. The proposed design is intended to operate principally between originating and terminating telecommunications switches. It can also be implemented on user devices. For calls passing through non-IP networks, the proposal carries the necessary CIV indicators and session identifier in the SS7 User-to-User Information parameter. The challenge itself is carried through the telephone-number field and the response through DTMF, both of which are supported across IP and traditional telephone networks. Legitimate organisational use of a presentation number can also be supported. For example, where a call centre

	presents its main switchboard number rather than an individual agent's number, verification calls to the main number must be routed to the system maintaining the state of outbound CIV calls. A central SIP proxy or equivalent service can perform this matching. Technical references: Current IETF Internet-Draft: Caller ID Verification in Heterogeneous Telecommunication Networks, draft-hao-civ-03 Peer-reviewed CIV research paper: "Spoofing Against Spoofing" The cited CIV document is presently an individual Internet-Draft. It is a work in progress, may be revised or replaced and has not yet been adopted or endorsed as an IETF standard.
Explain the advantages of the method.	It verifies control of the actual number displayed to the recipient. A caller spoofing a number that they do not control will not ordinarily receive the callback challenge and therefore cannot return the correct response. It does not require a global public-key infrastructure, certificate authorities or a central trusted third party. Verification relies on the telephone network's ability to route a callback to the claimed number. It can operate across heterogeneous networks, including SIP, cellular and traditional SS7-based networks. This is particularly significant while legacy and IP systems continue to coexist. It verifies the end-to-end displayed number rather than merely confirming that an upstream provider signed the information it received. It permits legitimate presentation-number arrangements. An organisation can present a central switchboard or customer-service number if its systems are configured to receive and answer CIV challenges for that number. Verification is automatic. The recipient does not need to hang up, manually enter the number or pay for a conventional callback. The verification state is short-lived and linked to a particular call using a session identifier, reducing the opportunity to reuse a response.

	It can be implemented in telecommunications switches, allowing verification to occur before the call causes the recipient's device to ring. It uses small messages and established signalling mechanisms. The proposed non-IP representation requires only approximately 17 bytes of User-to-User Information, while the response uses widely supported DTMF. It can make scammers more traceable. If calls using numbers that the caller does not control are rejected, scammers are pushed towards using numbers allocated to them. Subject to effective customer-identification and record-keeping requirements, the relevant range holder can then identify the subscriber or terminate the number. CIV can complement rather than replace other protections, including carrier authentication, customer due diligence, call analytics, Do Not Originate lists and STIR/SHAKEN.
Describe any disadvantages with using the method.	It verifies possession or control of the displayed telephone number. It does not prove the personal identity of the speaker, the name of an organisation or that the call is honest. A scammer using a number legitimately allocated to them could pass CIV. Its security model assumes that an ordinary attacker cannot intercept or redirect the automated callback. More capable attacks involving SIM swapping, SS7 compromise, unlawful interception or control of the destination number fall outside this assumption. Both sides of the call path need appropriate CIV support for a fully verified result. A caller can omit the CIV indicator or use a provider that does not support the system. This creates a downgrade risk, although the terminating provider can clearly label the number as unverified or restrict sensitive operations. Verification introduces additional signalling traffic because an extra, quickly terminated callback is generated for each checked call. The call must be held briefly while verification occurs. Although the draft anticipates a short delay, real-world latency should be measured under congestion, international routing and legacy-network conditions.

	A four-digit challenge has 10,000 possible values, giving a single random guess a probability of 1 in 10,000. Rate limits, detection of repeated failures and potentially longer challenges should be considered for high-risk applications. Call forwarding, SIP forking, private branch exchanges and distributed call centres require careful configuration so that the callback reaches the system maintaining the original call state. A malicious or incorrectly configured provider could generate verification calls that appear as missed calls on legacy devices. Networks should filter calls marked civ-veri-call and prevent them from reaching end users. Emergency calls should be exempt because any verification delay would be undesirable. The use of a modified presentation number to convey the challenge may require regulatory approval or specific treatment under national CLI rules. It should be formally reserved for network-generated CIV verification calls and should never be presented to an end user as an ordinary callable identity. The proposal requires interoperability testing to confirm that CIV information survives gateways, number normalisation, DTMF conversion, international transit and equipment from different vendors. The current specification is an individual Internet-Draft rather than an adopted IETF standard. Its protocol details may change, and the proposed header values have not yet completed the IETF standardisation and registration process.
Who owns the intellectual property rights to the method?	No response provided.
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of voice calls that you consider relevant.	No response provided.

A.2.2.6 The Fraud Victim Rights Organization

About You	
Your name	Tom Walker
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About Your Organisation	
The name and address of the organisation	The Fraud Victim Rights Organization
A brief description of the organisation's purpose	The Fraud Victim Rights Organization seeks to educate law enforcement and policy makers on the best ways to protect consumers from fraud and scams.
URL of the organisation's home page	fraudvictimrights.org
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls, 2. Methods to prevent the spoofing of the origin of text messages, 3. Methods to trace electronic communications to their origin
Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	No. Spoofing can contribute to fraud, but based on ten years of data, we now know reducing spoofing does not reduce fraud. Criminals will use legitimately subscribed phone numbers if they cannot spoof. In the United States, for example, in 2025 and 2026 only 25%-35% of scam calls were spoofed. The rest were made from legitimately subscribed phone numbers. Each country has different distributions of telecom networks, so the most cost effective ways to reduce spoofing vary by country.

	The first line of defense from spoofing is Do-Not-Originate (DNO). This prevents use of well known government or financial institution phone numbers. The second line is same-network caller ID validation. Though validating wireless subscribers while roaming through SS7 or Diameter can be costly to implement. The third line is blocking in-country caller IDs originating from another country. Though validating wireless subscribers while roaming through SS7 or Diameter can be costly to implement. Holistic caller ID validation through tokenization (such as the U.S. version of SHAKEN/STIR) takes decades to implement and has proven to be expensive and ineffective. Again, spoofing is not necessary for most phone scams.
Explain the advantages of the method.	Right fit for the right networks.
Describe any disadvantages with using the method.	There is considerable misinformation about how much fraud involves spoofing. Also, all counter-spoofing methods involve false positives.
Who owns the intellectual property rights to the method?	No one.
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of voice calls that you consider relevant.	Ten years of data conclusively show arrest and prosecution are the most efficient and effective ways to reduce phone scams.
Methods to Prevent the Spoofing of the Origin of Text Messages	
Do you recommend a particular method to prevent the spoofing of the origin of text messages?	Spoofing a caller ID through wireless networks is only possible if networks are incorrectly configured to sometimes not validate ANIs against MSISDNs in network HLRs and VLRs. This leaves spoofing through A2P. Restricting caller ID to assigned numbers on CPaaS platforms is simple to accomplish.

Explain the advantages of the method.	Simple to accomplish.
Describe any disadvantages with using the method.	An additional layer of regulatory control over CPaaS providers may be politically resisted.
Who owns the intellectual property rights to the method?	No one.
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of text messages that you consider relevant.	In countries where A2P spoofing is not allowed, most text message spam originates from SMTP-to-SMS gateways, SIM boxes with prepaid subscribers, and RCS. SIM box abatement requires law enforcement to track and seize SIM boxes. Stopping RCS spam requires changes to how Apple and Google manage end-to-end encryption.
Methods to Trace Electronic Communications to Their Origin	
Do you recommend a particular method (or methods) to trace the origin of electronic communications?	There is no particular method to tracing calls. Traceback is nothing more than the terminating provider contacting each provider in the call chain to determine the source of a call. Phone companies have been tracing calls to protect themselves and their customers for at least the past century.
Which kinds of electronic communication can be traced using the method(s)?	A2P SMS text message, iMessage text message, P2P SMS text message, RCS text message, Voice call to a telephone number, WhatsApp text message, WhatsApp voice call, Other over-the-top (OTT) communications
Explain the advantages of the method(s).	A2P SMS text message do not need to be traced, the originating number identifies the source. iMessage and Google Messages do not need to be traced, the originating number identifies the source. P2P SMS text message do not need to be traced, the originating number identifies the source. RCS text message do not need to be traced, the originating number identifies the source. Voice calls to a telephone number do not need to be traced unless spoofed.

	WhatsApp text message do not need to be traced, the originating number identifies the source. WhatsApp voice call do not need to be traced, the originating number identifies the source. Other over-the-top (OTT) communications do not need to be traced, the originating number identifies the source.
Describe any disadvantages with using the method(s).	None.
Who owns the intellectual property rights to the method(s)?	No one.
Provide any other insights into the methods that can be used to trace the origin of electronic communications that you consider relevant.	No response provided.

A.2.2.7 Professor Feng Hao

About You	
Your name	Professor Feng Hao
Are you answering this survey on behalf of an organisation or as a private individual?	As a private individual
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About You as a Private Individual	
Are you resident in a European Union country?	No
In which countries or territories do you have relevant experience of spoofing or traceback?	United Kingdom
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls
Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	Caller ID verification (CIV). Full details are here: https://www.ietf.org/archive/id/draft-hao-civ-03.html
Explain the advantages of the method.	Doesn't require any public key infrastructure or Certificate Authority: works with both IP and non-IP networks; simple to implement without involving a trusted third party.
Describe any disadvantages with using the method.	It involves a round trip to complete the challenge-response protocol
Who owns the intellectual property rights to the method?	The method was invented by researchers in the University of Warwick. It is published in the open domain and is not encumbered.
Provide any other insights into the methods that can be used to	No response provided.

prevent the spoofing of the origin of voice calls that you consider relevant.	

A.2.2.8 Heksagon

About You	
Your name	Muhammad Bilal Khan
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About Your Organisation	
The name and address of the organisation	Heksagon, Nedeljka Cabrinovica 62, 11030, Belgrade, Serbia
A brief description of the organisation's purpose	Software vendor building advanced fraud management, interconnect, and service monetization solutions for telecom operators and enterprises.
URL of the organisation's home page	www.heksagon.com
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls, 2. Methods to prevent the spoofing of the origin of text messages, 3. Methods to trace electronic communications to their origin
Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	Yes. Real-time Call Validation (CVS) at the interconnect, deployed as a module of the Heksagon Voice Firewall (https://www.heksagon.com/fraud-detection/real-time-protection/voice-firewall/call-validation). Heksagon launched one of the first Voice Firewalls in 2012 and was among the first vendors to develop and commercially deploy call validation outside North America. We introduced the concept to operators in 2018, implemented it with three of the four mobile operators in one national market, and openly shared the API with the fourth operator and with third parties; that API became the basis for the interoperability rules later

	adopted in national regulation. To our knowledge, ours was the first platform in commercial use to perform real-time call validation rather than single-operator checks. The solution operates at two complementary levels: • End-to-end, pre-call-setup validation: The Originating operator communicates directly with the target terminating operator to inform them about the originated call. In the notification variant, the originating operator announces the call setup in advance and the terminating operator matches the incoming call against that notification. Either way, the verdict exists before ring, so the spoofed call never reaches the subscriber. • Regional, inter-operator validation: The same mechanism applied across a national or regional group of operators located in a region or country, using assigned number-range and mobile number portability data to identify the correct home network. The Receiving operator identifies the home operator of the CLI and sends the request to validate the call. Only a minimal hashed identifier is exchanged: no CDR-level data or subscriber details leave the originating network. Neither method requires full IP migration or a national certificate infrastructure. Rules are configurable per route, per operator, and per number range, so calls can be validated, rerouted, anonymized, tagged or only logged. The same platform covers adjacent spoofing vectors such as SIMBOX bypass, fraudulent flash calls and robocalls, and supports bilateral and national call-verification schemes. The solution is proven in production with multiple global operators. Call validation approaches are country- or region-specific. Numbering plans, portability data, regulatory mandates and the state of IP migration differ from market to market, and no single national scheme transfers cleanly to another. Heksagon therefore supports both paths at once: deployment of a regional call validation solution, which can be in production in a given country or region within weeks, and integration with other platforms supporting in-band and out-of-

	band call verification, so that participating operators remain reachable from schemes built on different technical foundations. A market can act now on the spoofing problem it has today without foreclosing the option of adopting whichever global standard, or standards, ultimately prevails. Compliance and standards alignment: • Data protection: only hashed identifiers are exchanged, with no subscriber identity, call content, or location data crossing the interconnect, which keeps the GDPR assessment narrow and makes data minimization demonstrable. • Interoperability: interworks with STIR/SHAKEN and with GSMA frameworks such as Call Check and Open Connectivity/OVC where these already exist, complementing rather than replacing them. • Technology neutrality: works across 2G/3G/4G/5G over SS7/CAMEL, SIP/IMS, and open API, with no national PKI and no full IP migration required. • Open, published API and no vendor lock-in: any vendor's platform can be made interoperable, which is what allows a regulator to mandate an outcome rather than a supplier. • Operator sovereignty: the home network returns a verdict only; the decision to block, reroute, anonymize, tag or log always remains with the terminating operator and can be aligned to NRA rules, whitelists, and national exceptions. • Auditability: every query, response, and enforcement action is logged with a timestamp. A regulator or an interconnect partner can be shown the record rather than a claim about it. • Industry participation: Heksagon is an active contributor to multiple industry initiatives including GSMA and One Consortium. • Traceback capabilities: because each validation query and verdict is an independent, time-stamped record of whether a call was genuinely originated by the claimed subscriber, the same deployment doubles as a

	traceback source. Records held at each participating operator, or in the central node where one is used, are correlated on a common identifier and time window to reconstruct a call route hop by hop back to the originating network and to every transit carrier that accepted the traffic. Heksagon International Traceback (https://www.heksagon.com/fraud-detection/real-time-protection/voice-firewall/international-traceback) builds this into an evidence pack a regulator or law-enforcement body can act on, and a confirmed origin can be fed straight back into the firewall rules so that the next call from that route is blocked the same day.
Explain the advantages of the method.	• Open, not proprietary, no vendor lock-in: The validation protocol and API are published and freely implementable. Heksagon shared them openly with third-party operators and vendors from the outset, and competing platforms already interoperate with them. An operator or a regulator adopting the method is not tied to a single supplier, and a national scheme can be specified as an interface rather than as a product. • Fully technology-agnostic: The same validation logic runs over IP (SIP/IMS) and legacy protocols like SS7, and is also reachable over a plain REST API, so operators at any stage of IP migration participate on equal terms. It seamlessly works across 2G/3G/4G/5G with no national PKI and no handset, standards, or signaling dependencies. • Simple and easily scalable: A single query and a single response per call, with only a hashed identifier exchanged, means negligible added latency and a small integration footprint; deployment is measured in weeks rather than months. The distributed architecture scales horizontally, avoids a single point of failure, and grows incrementally: two operators can start bilaterally without waiting for a market-wide mandate, and each new participant increases coverage without redesign. • Effective without user dependency: Validation happens before call setup, so a spoofed call never reaches the subscriber. • Privacy-light and evidence-producing: Only hashed identifiers cross the interconnect, which

	simplifies GDPR assessment, while the query and verdict log yields evidence usable in regulatory and interconnect disputes.
Describe any disadvantages with using the method.	Effectiveness depends on adoption and participation of the majority of operators operating in the market.
Who owns the intellectual property rights to the method?	Heksagon Technology Ltd. (Belgrade, Serbia; www.heksagon.com) owns the intellectual property in its Voice Firewall and Call Validation implementation.
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of voice calls that you consider relevant.	No single method can fully solve spoofing. In our view, operators should be required to deploy real-time voice firewall solutions in their networks to combat CLI Spoofing. Voice firewall (VFW) solutions can greatly reduce CLI Spoofing threats and are, in our experience, a necessary basis for all advanced validation capabilities. Additionally, introducing Call Validation layer on top of deployed VFW solutions can completely eliminate CLI Spoofing, restoring trust in voice communications. We would encourage the EU to consider VFW deployment as a standard in EU countries. Also, evolution to advanced validation capabilities is possible using open-API-based interoperability interfaces rather than one named technology: a STIR/SHAKEN-only mandate would exclude the large share of EU traffic still originating on non-IP networks. Because validation is in practice country- or region-specific, we believe the pragmatic path is to deploy a regional validation solution quickly while requiring integration with platforms supporting in-band and out-of-band verification. That delivers protection in the near term and leaves the market fully prepared for a global standard should one emerge as prevailing.
Methods to Prevent the Spoofing of the Origin of Text Messages	
Do you recommend a particular method to prevent the spoofing of the origin of text messages?	Yes. An SMS Firewall at the international and A2P gateway, combined with a Signaling Firewall on SS7/Diameter (https://www.heksagon.com/fraud-detection/real-time-protection/sms-firewall) (https://www.heksagon.com/fraud-detection/real-time-protection/signaling-firewall). SMS differs structurally from voice here. A call crosses a chain of transit carriers, each able to rewrite the CLI, which is why voice

	requires an out-of-path query back to the claimed home network. An SMS is normally delivered end-to-end from the originating SMSC to the recipient's network, with SMS hubbing as the main exception, so the true origin is visible to the receiving operator in the signaling itself. The firewall compares the originating global title against the sender ID being claimed and the expected route for that sender, and blocks, silently drops, or transparently logs any message where the two do not match. Gray routes, SIM-farm traffic, and spoofed sender IDs are detected by pattern, volume, and content analysis rather than static blacklists alone. The signaling layer stops the MT-SMS injections, home-routing bypass, and SS7 exploits used to insert spoofed messages directly into the network.
Explain the advantages of the method.	Deployed at each operator's network core, the firewall screens every inbound message entering that network, whichever way it arrives: international gateways, domestic interconnects, A2P aggregator and SMPP connections, roaming partners, and direct enterprise links. Because verification happens at the receiving network, one operator's deployment protects that operator's subscribers immediately, with no dependence on any other operator participating. It works on existing SMSC infrastructure with no handset or standards change. A registered sender-ID scheme is enforceable and auditable: every alphanumeric sender has a named, contactable owner. Blocking happens before delivery, so the subscriber never sees the message. The same platform produces the evidence needed to act against the aggregator that injected the traffic.
Describe any disadvantages with using the method.	Registries of alphanumeric brand sender IDs need governance, a dispute process, and cross-border recognition. Otherwise, a brand registered in one member state remains spoofable from another. Over-blocking can stop legitimate enterprise traffic, so exception handling matters. The firewall is blind to attacks like the emerging SMS blasters, which transmit directly over the air, and to OTT messaging. Encrypted or obfuscated content limits content-based rules. Finally, continuous tuning is required as fraudsters rotate sender IDs and routes.

Who owns the intellectual property rights to the method?	Heksagon Technology Ltd. owns the intellectual property in its SMS Firewall and Signaling Firewall products.
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of text messages that you consider relevant.	Because SMS origin is verifiable at the receiving network, an EU measure here would not need a new inter-operator scheme, a standard, or a certificate infrastructure. Requiring operators to run the originating-address check and to act on mismatches is deployable now, on equipment many networks already have. That would make SMS the cheaper of the two problems to legislate for. However, fraud migrates. Tighten A2P SMS and the traffic moves to flash calls, to RCS, or to OTT platforms, so any EU measure would be better assessed against channel shift than judged on SMS volumes alone. RCS is arriving with brand verification built in and is worth addressing early, while the ecosystem is still small. We would also flag that one of the fastest-growing spoofing vectors we currently see is hardware-based: SMS blasters broadcasting from vehicles. That is a spectrum and enforcement problem rather than a filtering one, and no gateway rule reaches it. Equipment import controls and radio-layer detection would largely contribute to fraud prevention.
Methods to Trace Electronic Communications to Their Origin	
Do you recommend a particular method (or methods) to trace the origin of electronic communications?	Yes. Tracing is built on records operators already hold, correlated on a common identifier and time window. Heksagon addresses it per channel: • Voice: Heksagon International Traceback (https://www.heksagon.com/fraud-detection/real-time-protection/voice-firewall/international-traceback) reconstructs a call route hop by hop, from the terminating operator back through each transit carrier to the originating network. Two further sources make that reconstruction verifiable: Call Validation (CVS) records, where each hashed query and verdict is an independent, time-stamped record of whether the claimed subscriber actually originated the call, and Test Call Generation (https://www.heksagon.com/fraud-detection/real-time-protection/test-call-generation), which places controlled calls over a suspect route to

	prove empirically which CLI is delivered and at which hop it is altered. • SMS: message-level records from the SMS Firewall together with SS7/Diameter signaling logs identify the injecting aggregator, gateway and inbound interconnect for A2P and P2P traffic, so a spoofed sender ID can be correlated back to the submitting SMPP account and its contractual owner. • Other channels (data, IP and OTT): IPDR (https://www.heksagon.com/network-services/ipdr) consolidates CGNAT, AAA/RADIUS, GTP and DPI metadata into a single retained record set, mapping an IP session and its NAT translation back to a subscriber line and linking IP sessions to the corresponding voice and SMS events. This reaches OTT calls and messages, where there is no interconnect signaling to trace. In every case, the output is an evidence pack with a documented chain of custody, built for a regulator or law-enforcement body to act on.
Which kinds of electronic communication can be traced using the method(s)?	A2P SMS text message, iMessage text message, P2P SMS text message, RCS text message, Voice call to a telephone number, WhatsApp text message, WhatsApp voice call, Other over-the-top (OTT) communications, IP data sessions, traced via IPDR and NAT logs
Explain the advantages of the method(s).	All of these methods are deployed seamlessly in telco operators following international standards, so none requires a change to signaling or handsets. They are deployable operator by operator and get better as more participants join. • Traceback identifies the origin and every transit carrier that accepted the bad traffic, which is where commercial pressure works best. It produces an end-to-end auditable chain of custody suitable for regulatory and criminal proceedings. Once a gray source/route is identified, it can be blocked at the firewall the same day. • Call validation records give an independent, real-time answer on whether the claimed subscriber originated the call.

	• Test call generation supplies empirical proof of what a route actually does with CLI, which converts a disputed traceback into a demonstrable fact in an interconnect dispute. • IPDR extends the same approach to IP and OTT traffic by mapping a session and its NAT translation back to a subscriber line, and correlates IP sessions with voice and SMS events so a single subscriber view spans all channels.
Describe any disadvantages with using the method(s).	The main limitations differ by method: • For traceback, manual request handling makes cases take days or weeks, which is too slow for live fraud, and records must be retained long enough to correlate. • Call validation records only exist for calls between operators that participate in a scheme, so coverage follows adoption.
Who owns the intellectual property rights to the method(s)?	Heksagon Technology Ltd. owns the intellectual property in its International Traceback and IPDR products.
Provide any other insights into the methods that can be used to trace the origin of electronic communications that you consider relevant.	In our opinion, what limits traceback in Europe today is procedural rather than technical. We would suggest the EU consider: • a mandatory response obligation with a fixed deadline (24 to 48 hours) on any carrier terminating traffic into the Union • a per-operator single point of contact register • a standard machine-readable request and response format so traceback can be automated rather than emailed • a harmonized lawful basis and minimum retention period for the specific fields traceback needs • consequences for transit carriers that repeatedly cannot identify their upstream • country or regional agent supporting traceback - assuring eligibility of requests and facilitating the international part of the procedures (preventing misuse)

	Controlled automation can turn traceback from forensics into prevention. At machine speed, a confirmed origin can feed straight back into the firewalls that block the next call.

A.2.2.9 jtendo

About You	
Your name	Michał Wachowiak
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About Your Organisation	
The name and address of the organisation	jtendo, 8C Pelplinska, 01-683 Warsaw, Poland
A brief description of the organisation's purpose	jtendo provides solutions and services to Mobile Network Operators. We are experts in network signaling, network security, application development, integration, deployment and solution support.
URL of the organisation's home page	https://jtendo.com/
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls
Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	No single method is enough on its own. CLI spoofing has to be handled in layers, combining controls that run from the simplest and most static to the most advanced: - Do Not Originate (DNO) lists - block calls from numbers that should never originate a call: inbound-only, invalid, unallocated, unused, and emergency, government or financial lines. - Allow and block lists - dynamic filtering of trusted and suspicious numbers and patterns, ideally pattern-based (prefix/regex) and supported by AI/ML.

	- Location check - HLR/VLR verification that confirms whether one of our own subscribers, presented as the calling party on interconnect, is really roaming. If not, the call is spoofed. - Roaming on-call check - CAMEL/CAP call-context analysis that confirms a roaming subscriber actually originated the call. - Inter-operator API - a real-time query to the number's home operator to confirm whether the calling party is legitimate. Each layer covers cases the one below it cannot. The method we recommend as the final and decisive one - described in full below, and the basis for our answers to the rest of the survey - is the inter-operator API. It is the only method that can validate a CLI belonging to another operator, and that is the highest-risk case: the most damaging spoofing arrives on international interconnect carrying the number of a domestic subscriber of a different operator. Location and roaming checks are unilateral, so they cover only our own subscribers. Static lists cannot judge an ordinary number that is originating legitimately. Only a query to the number's home network gives a conclusive answer. The inter-operator API validates the calling party number of a call arriving from an untrusted source, for example an international trunk. When an MNO receives such a call and the CLI belongs to another operator in the same country, it queries that operator's API in real time to ask whether the subscriber is roaming and whether they really originated the call. The response classifies the call as spoofed, legitimate, or uncertain and in need of further checks. The queried operator answers using whichever internal method fits its own infrastructure, usually the location check or the roaming on-call check described above, so the API exposes those layers across network boundaries. Transport can be REST or gRPC; what matters is that every operator exposes the same functionality in the same way. Our main recommendation is that this should be a properly standardised inter-operator API. Today it exists

	nationally in a handful of countries, operator to operator, but each deployment uses its own interface definition and semantics. There is no common cross-operator standard, and that is the core limitation: the worst spoofing enters on cross-border links, so an API scoped to one country and defined differently in each one cannot reach the interconnects where the fraud actually originates. The industry should converge on a single profile built on GSMA Open Gateway and the CAMARA number-verification and KYC API families, so that verification works between countries as well as inside them.
Explain the advantages of the method.	- It is the only method that can validate a number belonging to another operator, and it returns a definitive spoofed or legitimate verdict that supports immediate blocking or alerting. - It covers the highest-risk vector, spoofed domestic numbers arriving on international interconnect, which unilateral methods cannot reach at all. - It aggregates the other layers. The responding operator can use its location or roaming check internally, so the API is as strong as the best control each participant runs. - It can be standardised through GSMA Open Gateway and CAMARA, works over REST or gRPC, and runs in real time before or during call setup.
Describe any disadvantages with using the method.	- It requires cooperation, mutual trust and commercial and legal agreements between operators. This is the hardest part to get started. - Fragmentation today: national interfaces differ, so there is no cross-border interoperability yet. This is the main gap standardisation has to close. - Every operator has to expose and maintain the API to an agreed SLA for availability and latency, which adds operational work and consumes part of the call-setup latency budget. - Sharing subscriber presence and roaming status raises privacy and regulatory questions, particularly across jurisdictions.

	- "Uncertain" responses need defined fallback logic: monitor, flag, or route to another check.
Who owns the intellectual property rights to the method?	The method is not owned by any single private party. It is an open cross-operator practice, and the vehicles it should build on are openly specified (GSMA Open Gateway) or open source (CAMARA, under the Linux Foundation). Where the method is deployed nationally, the individual operator interfaces and any bespoke orchestration belong to those operators and their vendors. Commercial IP sits in the specific product implementations, not in the concept.
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of voice calls that you consider relevant.	We have production deployment experience with this method: we implemented and launched the inter-operator verification system in Poland across all four major mobile network operators. That gives us direct insight into the operational and governance problems the survey may be interested in - interface definition and message semantics, latency budgets in the call-setup path, response classification (spoofed, legitimate, uncertain) and fallback handling, and the inter-operator agreements needed to make cross-network querying work. If any of the following answers would be more useful with implementation-level detail, we can provide it.

A.2.2.10 Magrathea Telecommunications Ltd

About You	
Your name	Name withheld at respondent's request
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I want my name to be omitted from the report of the survey findings.
About Your Organisation	
The name and address of the organisation	Magrathea Telecommunications Ltd
A brief description of the organisation's purpose	Wholesale carrier
URL of the organisation's home page	www.magrathea-telecom.co.uk
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls, 3. Methods to trace electronic communications to their origin
Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	Visibility of number 'ownership' to enable validation checks
Explain the advantages of the method.	We should try accessible methods before the disruptive costly ones
Describe any disadvantages with using the method.	Still leaves gaps, but it's a start
Who owns the intellectual property rights to the method?	Nobody
Provide any other insights into the methods that can be used to	An effective trace back would be a good deterrent

prevent the spoofing of the origin of voice calls that you consider relevant.	
Methods to Trace Electronic Communications to Their Origin	
Do you recommend a particular method (or methods) to trace the origin of electronic communications?	I am only familiar with the US Traceback model and the basic model used in the UK. The UK one is not good enough or accessible enough. US model appears to be effective.
Which kinds of electronic communication can be traced using the method(s)?	Voice call to a telephone number, Not sure but expect others are now included
Explain the advantages of the method(s).	Simple and effective
Describe any disadvantages with using the method(s).	Requires central authority to manage
Who owns the intellectual property rights to the method(s)?	No response provided.
Provide any other insights into the methods that can be used to trace the origin of electronic communications that you consider relevant.	CP registry, having awareness of who operates in this space would be useful

A.2.2.11 NeoSoft AG

About You	
Your name	Name withheld at respondent's request
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I want my name to be omitted from the report of the survey findings.
About Your Organisation	
The name and address of the organisation	NeoSoft AG, Uetlibergstrasse 132, 8045, Zurich, Switzerland
A brief description of the organisation's purpose	The company provides government organizations with state-of-the-art technologies and tools designed to support intelligence gathering from cellular networks and enhance protection against cellular network threats.
URL of the organisation's home page	https://www.neosoft.ch/
Areas of Contribution	
Do you wish to contribute your insights about:	2. Methods to prevent the spoofing of the origin of text messages
Methods to Prevent the Spoofing of the Origin of Text Messages	
Do you recommend a particular method to prevent the spoofing of the origin of text messages?	NeoSoft provides a portable, handheld solution for real-time detection and geolocation of SMS blasters, called BTS Hunter. When entering the operational range of a fake cell tower, such as an SMS blaster, BTS Hunter immediately alerts the operator and accurately identifies active SMS-blaster transmissions across all network providers (PLMN) and cellular technologies, from 2G through 5G-SA. BTS Hunter can also assist operators in locating the source of the transmission using a directional-finding

	approach. This capability enables the operator to precisely narrow down the source to a specific individual within a crowd or to a vehicle in which the SMS blaster is concealed. P.S. I am unable to attach the product brochure, as the submission form doesn't allow for files to be attached. Please contact us to [contact detail omitted] for more details.
Explain the advantages of the method.	BTS Hunter complements telco-provider-based detection systems that identify the presence of fake cell towers by analyzing signaling patterns within the network. These approaches provide network-level visibility, yet they face several practical limitations. BTS Hunter addresses these limitations through direct, passive RF monitoring: 1. Signaling-based approaches traditionally involve delays of up to 15 minutes before relevant data reaches the core network. Solution: BTS Hunter can detect a fake cell tower within 60 seconds of the start of its transmission, while BTS Hunter Pro can reduce the detection time to as little as 5 seconds. 2. SMS blasters can rapidly change their broadcasted PLMN and radio technology, including switching between 2G, 3G, 4G, and 5G. Tracking such devices across multiple network cores and providers is highly challenging from a coordination perspective and may require cooperation between multiple network operators and radio cores. Solution: BTS Hunter is provider- and technology-agnostic, passively monitoring the RF environment and identifying transmissions from fake cell towers regardless of the network provider or radio technology being used. 3. Provider-based systems can identify an area in which an SMS blaster is operating, but precisely locating the source of the transmission remains challenging.

	Solution: BTS Hunter features directional-finding capability designed to precisely location the transmission source with sub-meter level accuracy. 4. From a signaling perspective, IMSI catchers and SMS blasters can generate similar traces, making it difficult for provider-based systems to determine whether a detected signaling anomaly originates from a legitimate law-enforcement operation involving an IMSI catcher or from a maliciously deployed SMS blaster. Solution: BTS Hunter offers an optional capability to identify the manufacturer of equipment associated with detected fake cells, providing an additional layer of intelligence to help distinguish known, authorized LEA equipment from potentially unauthorized SMS-blaster deployments.
Describe any disadvantages with using the method.	Even when using BTS Hunter, accurately locating an SMS blaster remains logistically challenging when the attacker is inside a moving vehicle. To address this challenge, we are exploring a new concept for efficiently identifying and tracking such vehicles. The proposed approach combines strategically positioned, rapidly scanning RF sensors with real-time CCTV footage to cross-correlate multiple detections and footages, enabling to identify the exact vehicle. The approach is in the conceptual stage and it's effectiveness has not yet been validated in operational conditions.
Who owns the intellectual property rights to the method?	NeoSoft AG
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of text messages that you consider relevant.	No response provided.

A.2.2.12 NG-BLU Networks

About You	
Your name	Jeff Bremer
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About Your Organisation	
The name and address of the organisation	NG-BLU Networks, Wethouder Wassebaliestraat 6c, 7951 SN Staphorst, Netherlands
A brief description of the organisation's purpose	Wholesale networks and telecommunication
URL of the organisation's home page	https://www.ngblu.nl
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls, 3. Methods to trace electronic communications to their origin
Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	No response provided.
Explain the advantages of the method.	No response provided.
Describe any disadvantages with using the method.	No response provided.
Who owns the intellectual property rights to the method?	No response provided.
Provide any other insights into the methods that can be used to	No response provided.

prevent the spoofing of the origin of voice calls that you consider relevant.	
Methods to Trace Electronic Communications to Their Origin	
Do you recommend a particular method (or methods) to trace the origin of electronic communications?	No response provided.
Which kinds of electronic communication can be traced using the method(s)?	No response provided.
Explain the advantages of the method(s).	No response provided.
Describe any disadvantages with using the method(s).	No response provided.
Who owns the intellectual property rights to the method(s)?	No response provided.
Provide any other insights into the methods that can be used to trace the origin of electronic communications that you consider relevant.	No response provided.

A.2.2.13 NICC Standards Limited

About You	
Your name	Nick Ireland
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About Your Organisation	
The name and address of the organisation	NICC Standards Limited
A brief description of the organisation's purpose	UK telecommunications standards body
URL of the organisation's home page	https://niccstandards.org.uk/
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls, 2. Methods to prevent the spoofing of the origin of text messages, 3. Methods to trace electronic communications to their origin
Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	Still under investigation within NICC and its member organisations
Explain the advantages of the method.	Still under investigation within NICC and its member organisations
Describe any disadvantages with using the method.	Still under investigation within NICC and its member organisations
Who owns the intellectual property rights to the method?	Any solution must be a public solution so there will be no IPR

Provide any other insights into the methods that can be used to prevent the spoofing of the origin of voice calls that you consider relevant.	Still under investigation within NICC and its member organisations
Methods to Prevent the Spoofing of the Origin of Text Messages	
Do you recommend a particular method to prevent the spoofing of the origin of text messages?	Still under investigation within NICC and its member organisations
Explain the advantages of the method.	Still under investigation within NICC and its member organisations
Describe any disadvantages with using the method.	Still under investigation within NICC and its member organisations
Who owns the intellectual property rights to the method?	Any solution must be a public solution so there will be no IPR
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of text messages that you consider relevant.	Still under investigation within NICC and its member organisations
Methods to Trace Electronic Communications to Their Origin	
Do you recommend a particular method (or methods) to trace the origin of electronic communications?	Still under investigation within NICC and its member organisations
Which kinds of electronic communication can be traced using the method(s)?	Still under investigation within NICC and its member organisations
Explain the advantages of the method(s).	Still under investigation within NICC and its member organisations
Describe any disadvantages with using the method(s).	Still under investigation within NICC and its member organisations
Who owns the intellectual property rights to the method(s)?	Any solution must be a public solution so there will be no IPR
Provide any other insights into the methods that can be used to	Still under investigation within NICC and its member organisations

trace the origin of electronic communications that you consider relevant.	

A.2.2.14 Oculeus GmbH

About You	
Your name	Arnd Baranowski
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About Your Organisation	
The name and address of the organisation	Oculeus GmbH, Friedensstraße 6-10, 60311 Frankfurt am Main, Germany
A brief description of the organisation's purpose	Oculeus is an international provider of software solutions to telecoms carriers. Anti-fraud and verification systems are a major part of our product suite.
URL of the organisation's home page	https://www.oculeus.com
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls, 2. Methods to prevent the spoofing of the origin of text messages, 3. Methods to trace electronic communications to their origin
Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	Oculeus 2FN, previously called GSMA Call Check, is a universal multi-channel system for authenticating the origin of all communications, including voice calls, over any kind of network. The name was changed to reflect the fact that the system can also be used to verify the origin of SMS, RCS, iMessage, WhatsApp etc. All that is required is for the originating and terminating carriers to adopt an instance of our software that runs as a node in the cloud, and then to exchange data with their own node via an API. Each carrier's node then exchanges data with the nodes of other carriers, providing a

	parallel out-of-band network to the network used for the transmission of the customer's communication. We refer to this as a 'two factor network' (2FN) because the nodes operate as a second network to validate information received by the carriers' own networks and to highlight discrepancies such as CLI spoofing and other methods used for fraud. The cryptographic security of the system has been validated by the GSMA and Secure Research Labs (SRLabs), a leading German telecoms cybersecurity consultancy. The system is designed with privacy in mind, using a decentralized architecture that never stores information for longer than is required for the exchange of data with other nodes. Users are also free to set limits on the kinds of information they will share using the nodes, and which other carriers they will share that information with. More information about Oculeus 2FN can be found here: https://www.oculeus.com/products/oculeus-2fn
Explain the advantages of the method.	It can be used for any type of communication across any type of electronic network. it is cost-effective and quick to implement because users only need to run an instance of the software in the cloud and to integrate with the node via an API that speaks to their internal systems. It has security and privacy-by-design because data is not centralized and is only retained as long as necessary to perform the exchange between carrier nodes. It works independently of the network being used to carry the communication being authenticated, so can be used to authenticate communication over any kind of network or any combination of networks. It only requires the consent and cooperation of the originating and terminating carriers because there is no reliance on intermediate carriers to transmit any data. This means there is no possibility of interference by intermediate parties/countries as 2FN works completely independently of the national or international routing of any communication it authenticates. It can also be used for traceback if carriers decide to retain the data they obtain from their node as proof of the origin of communications they receive. It can also be used for roaming status checks within a country to prevent spoofing of domestic mobile numbers even if foreign carriers do not adopt 2FN

	because this only requires domestic carriers to exchange data about the roaming status of their own customers. The multi-purpose design and the use of nodes in the cloud mean the system is highly extensible, so if carriers in one country adopt 2FN for one purpose, and carriers in a neighboring country adopt 2FN for a different purpose, it is a simple matter for those countries to 'switch on' the exchange of data for different purposes or to exchange data with each other when they decide they want to do that.
Describe any disadvantages with using the method.	The system relies on the cooperation of the originating and terminating carrier to exchange data but that is a limitation inherent to all authentication protocols. Telemarketing capabilities, such as using 2FN to also transmit an OVC or SHAKEN signature, should be possible in principle but have not been thoroughly tested so far. The ultimate effectiveness of 2FN depends on how many carriers use it at the same time.
Who owns the intellectual property rights to the method?	Oculeus GmbH
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of voice calls that you consider relevant.	2FN was devised in consultation with the GSMA to provide a low-cost solution for call validation but the method is just as suited to authenticating other communications too. The GSMA removed their brand from the product because of their need to remain 'neutral' with respect to alternative solutions for authenticating and tracing communications but we still believe this is the simplest, cheapest and safest method that would deliver authentication and traceback capabilities within Europe, and with European-grade security and privacy, in the least possible time.
Methods to Prevent the Spoofing of the Origin of Text Messages	
Do you recommend a particular method to prevent the spoofing of the origin of text messages?	Oculeus 2FN, see the answer above. The architecture of 2FN nodes exchanging data works just as well when transmitting data about SMS, RCS and other text messages. Businesses like SMS aggregators would just need to adopt their own nodes and to talk to them via APIs like any other communications provider.

Explain the advantages of the method.	See answer above. Also, the same system can be used to authenticate and trace voice calls, any OTT communication etc.
Describe any disadvantages with using the method.	See answer above.
Who owns the intellectual property rights to the method?	Oculeus GmbH.
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of text messages that you consider relevant.	We believe our solution is the only working solution that authenticates text messages using any protocol just as well as authenticating voice calls.
Methods to Trace Electronic Communications to Their Origin	
Do you recommend a particular method (or methods) to trace the origin of electronic communications?	See the answer above. The security and privacy-oriented design of 2FN means it was not designed to retain data but the goal of traceback can easily be attained by either mandating terminating carriers to retain evidence that the origin of a communication was authenticated or by adding a node so that a law enforcement agency receives a copy of authentication for its own records. Then traceback to the origin of a communication becomes a trivial matter of looking up the data from a database of authenticated communications.
Which kinds of electronic communication can be traced using the method(s)?	A2P SMS text message, iMessage text message, P2P SMS text message, RCS text message, Voice call to a telephone number, WhatsApp text message, WhatsApp voice call, Other over-the-top (OTT) communications, Any electronic communication where the originating and terminating communications provider have implemented data sharing with each other via a 2FN node
Explain the advantages of the method(s).	Traceback using 2FN cannot be obstructed by any technological or legal means so long as the originating and terminating carriers enable the exchange of data through 2FN. This means it cannot be affected by changes in network routing, network technology, laws relating to networks and data sharing for any of the intermediate carriers that may be involved in transmitting an international communication. This

	'immediate' method, which links the communication immediately to its origin, is hence superior to the methods that involve identifying every intermediate carrier and tracing the communication through every intermediate carrier. Tracing through intermediate carriers is risky because the trace will not be completed if any of them are unable or refuse to support the method because of technological limitations of how their networks work or legal limits on what data they are allowed to share.
Describe any disadvantages with using the method(s).	2FN traceback provides no data about the route that a communication took. This is only a disadvantage if the goal of traceback is to punish intermediate carriers for not blocking traffic. For example, if an illegal voice call was made from Cambodia to Belgium via a carrier in Germany then the German carrier might be punished for not blocking the call before it reached Belgium. Whether this is required is a question about law enforcement objectives, not about the quickest and simplest way to trace a communication to its origin.
Who owns the intellectual property rights to the method(s)?	Oculeus GmbH.
Provide any other insights into the methods that can be used to trace the origin of electronic communications that you consider relevant.	There is a big difference in the design of systems that trace a communication immediately to its origin (simpler, quicker, harder to interrupt) and systems that trace a communication through all intermediate carriers (more complex, slower, easier to interrupt, but more data about the route taken by the communication) but the question about which is needed for law enforcement depends on whether the goal is to identify the criminals responsible for originating the communication or enforcing obligations on intermediate communications providers. That is not a technological question but a matter for the requirements of the users -- the police and prosecutors.

A.2.2.15 Teleindustrien - Telecom Industry Association Denmark

About You	
Your name	Jakob Willer
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About Your Organisation	
The name and address of the organisation	Teleindustrien - Telecom Industry Association Denmark
A brief description of the organisation's purpose	Representing the Telecom Industry in Denmark
URL of the organisation's home page	teleindu.dk
Areas of Contribution	
Do you wish to contribute your insights about:	1. Methods to prevent the spoofing of the origin of voice calls, 2. Methods to prevent the spoofing of the origin of text messages
Methods to Prevent the Spoofing of the Origin of Voice Calls	
Do you recommend a particular method to prevent the spoofing of the origin of voice calls?	An international call arrives with an A-number belonging to the domestic numbering plan. The terminating operator queries the operator that owns/hosts that A-number to determine its current status. If the subscriber is roaming abroad, an internationally originated call with that A-number can be legitimate. If the subscriber is currently on the home network, the call should not normally be arriving from an international interconnect with that domestic A-number.

	The mismatch therefore provides a strong indication that the A-number has been spoofed, allowing the call to be blocked, flagged, or otherwise treated as suspected fraud.
Explain the advantages of the method.	Simple solution. Requires legislation that allows operators to exchange information about their customers
Describe any disadvantages with using the method.	There will still be cases that operators can not check. And the solution can be used to verify if a certain number is in the country or not.
Who owns the intellectual property rights to the method?	No response provided.
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of voice calls that you consider relevant.	No response provided.
Methods to Prevent the Spoofing of the Origin of Text Messages	
Do you recommend a particular method to prevent the spoofing of the origin of text messages?	List of protected sender IDs distributed among MO - legitimate source = allow - other sources = deny
Explain the advantages of the method.	Simple solution
Describe any disadvantages with using the method.	Does not protect against look alikes
Who owns the intellectual property rights to the method?	No response provided.
Provide any other insights into the methods that can be used to prevent the spoofing of the origin of text messages that you consider relevant.	No response provided.

A.2.2.16 USTelecom Industry Traceback Group

About You	
Your name	John Ayers
Are you answering this survey on behalf of an organisation or as a private individual?	On behalf of an organisation
Do you consent to your name being included in the report of the survey findings to be provided to the EU, or do you want your name to be omitted?	I consent to my name being included in the report of the survey findings.
About Your Organisation	
The name and address of the organisation	The Industry Traceback Group (ITG)
A brief description of the organisation's purpose	The ITG is designated by the U.S. Federal Communications Commission as the official consortium to lead private traceback efforts in the U.S. The ITG is also focused on working with other jurisdictions to deploy traceback capabilities. Additional information is available through the Industry Traceback Group Response to the European Commission Call for Evidence: Fighting Online Fraud – Action Plan Ref. Ares(2026)783547 available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16313-Fighting-online-fraud-action-plan/F33380254_en
URL of the organisation's home page	https://tracebacks.org
Areas of Contribution	
Do you wish to contribute your insights about:	3. Methods to trace electronic communications to their origin
Methods to Trace Electronic Communications to Their Origin	
Do you recommend a particular method (or methods) to trace the origin of electronic communications?	For voice calls, the ITG uses a traceback process that follows a call from the terminating provider upstream through the call path to identify the originating provider and, where available, the originating customer.

	The ITG manages tracebacks through its Secure Traceback Platform. Each provider identifies the upstream provider from which it received the traffic, allowing the traceback to proceed provider by provider through the call path. Providers respond either manually through the Secure Traceback Platform or via an API. The ITG incorporates available information, including STIR/SHAKEN authentication information, as part of the traceback record. The ITG's methodology and governance framework are described in its published Policies and Procedures at https://tracebacks.org/.
Which kinds of electronic communication can be traced using the method(s)?	Voice call to a telephone number
Explain the advantages of the method(s).	Traceback provides information about the provider path over which a call traveled and can identify the provider that originated the traffic. That information is distinct from, and can complement, call-authentication information. The ITG's experience also demonstrates value beyond an individual investigation. Traceback information can help providers identify recurring issues associated with customers or upstream providers and can inform customer vetting, Know Your Customer, Know Your Upstream Provider, and other risk-management and mitigation efforts.
Describe any disadvantages with using the method(s).	The ITG's traceback process relies on providers cooperating and accurately reporting information to the ITG. A traceback may not reach the originating provider where relevant information is unavailable or a provider does not cooperate. Even in those circumstances, including where information provided during the traceback is inaccurate or incomplete, the process can still provide information useful to investigation or mitigation.
Who owns the intellectual property rights to the method(s)?	The ITG operates the Secure Traceback Platform used to administer its traceback process.
Provide any other insights into the methods that can be used to	Based on the ITG's experience operating traceback, an effective traceback program can support disruption and

trace the origin of electronic communications that you consider relevant.	mitigation of unlawful traffic as well as investigation and enforcement. Its effectiveness depends on reliable sourcing of relevant call examples, sufficient scale to identify recurring patterns and actors, and a consistent process and operation. For disruption, traceback supports it by making providers aware of suspected unlawful traffic that originated on or traversed their networks, enabling them to investigate and, where appropriate, mitigate that traffic. Over time, traceback information can also inform providers' customer and upstream-provider risk management. Traceback and call authentication serve complementary functions. Traceback can support authentication efforts, including by identifying apparent instances in which calls may have been improperly authenticated, while also providing value in circumstances where calls are authenticated but the underlying traffic is nevertheless unlawful.