

METHODS TO FACILITATE THE TRACEBACK AND MITIGATE THE SPOOFING OF TELECOMMUNICATIONS

An External Expert Report prepared for ENACT

Main Author: Eric Priezkalns

Contributor: James Greenley





ABOUT ENACT

ENACT is a knowledge network focused on the fight against crime and terrorism (FCT). The network is funded under the Horizon Europe Framework Programme in Cluster 3 – Civil Security for Society. The project addresses the call topic HORIZON-CL3-2022-SSRI-01-02 ‘Knowledge Networks for Security Research & Innovation’, aiming to collect, aggregate, process, disseminate and make the most of the existing knowledge in the FCT area.

The project aims to satisfy two major ambitions,

- Provide evidence-based support to the decision-makers in the EU research and innovation (R&I) ecosystem in the FCT domain, targeted explicitly at enabling more effective and efficient programming of EU-funded R&I for the fight against crime and terrorism.
- Act as a catalyst for the uptake of innovation by enhancing the visibility and reliability of innovative FCT security solutions.



**Funded by
the European Union**

REPORT FEEDBACK

We're collecting feedback on this report through the EU Survey Platform, if you'd like to share your thoughts anonymously please click on the link below.

<https://ec.europa.eu/eusurvey/runner/enact-report-feedback>

COPYRIGHT

This report contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

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.

TRANSPARENCY & DISCLAIMER STATEMENT

This statement is provided for transparency purposes, **highlighting possible conflicts 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.

ACKNOWLEDGEMENT

This report was requested through ENACT's External Cooperation Pillar by Europol's European Cybercrime Centre (EC3) to analyse existing and operational technical solutions to mitigate Caller-ID and Sender-ID spoofing.

ACRONYMS

A2P	Application-to-Person
CHAKEN	Caller Identity Authentication Using Crypto Tokens (official English language abbreviation of the Chinese name)
CIV	Caller ID Verification
CLI	Calling Line Identification
CP	Communication Provider
E2EE	End-to-End Encryption
eIDAS	Electronic IDentification, Authentication and trust Services
EU	European Union
FCT	Fight against Crime and Terrorism
GDPR	General Data Protection Regulation
GLEIF	Global Legal Entity Identifier Foundation
GSMA	Global System for Mobile Communications Association
IP	Internet Protocol
ITU	International Telecommunication Union
KYC	Know Your Customer
LEA	Law Enforcement Agency
LEI	Legal Entity Identifier
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
OCS	Online Communication Service
OOB	Out of Band
OTT	Over-the-Top
OVC	Open Verified Communications
P2P	Person-to-Person
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
RBM	RCS Business Messaging
RCS	Rich Communication Services
SSI	Self Sovereign Identity
SHAKEN	Signature-based Handling of Asserted Information Using toKENs
SIP	Session Initiation Protocol
SMS	Short Message Service
SS7	Signalling System 7
STIR	Secure Telephone Identity Revisited
TDM	Time-Division Multiplexing
vLEI	Verifiable Legal Entity Identifier
VoIP	Voice over Internet Protocol

EXECUTIVE SUMMARY

The tracing of communications is used to fight many kinds of crime, but its effectiveness depends on the resources that law enforcement agencies (LEAs) can dedicate to acting upon intelligence supplied by communication providers (CPs). China has extradited many thousands of scammers from overseas call centres despite not asking foreign countries to build new systems to facilitate traceback. The USA's strategy concentrates on technology, including heavy expenditure on systems that facilitate traceback. However, the resulting number of prosecutions has been modest despite large volumes of scam calls originating on major US networks and a continued rise in the amounts lost by American consumers to scams instigated by a phone call. Europe can draw lessons from the different approaches adopted by China and the USA, including their respective strengths and limitations. In turn, Europe has much to teach the rest of the world about its own successes in tackling scams.

There is some ambiguity in what different parties mean when they discuss traceback. This leads to confusion about what is required of a traceback system. Solutions are designed incorrectly if there is no clear statement of requirements. Several respondents to our survey noted that traceback essentially involves asking CPs where a communication came from, per the records they retained. Countries have been tracing communications for many years. So, when considering how to implement a new system, we should ask what we are trying to trace, where we expect to trace it to, and what is deficient with the systems to be replaced.

The notion that a global traceback system stems from work on an allied problem: the authentication of communications. 'Authentication' is a way of saying work has been done to prevent impersonation. Much of this work is imperfect. This report links the questions of how to tackle spoofing with how to trace communications. Tracing is more general in application. And if we know the origin of a communication with certainty, because it has been authenticated and the sender was subject to rigorous know-your-customer (KYC) checks, then 'tracing' that communication is just a peculiar way of saying we look at the sender's address per the communication. Chapter 5 of this report evaluates 15 methods for authentication or tracing (or both). Considering all the options helps to clarify the strengths and weaknesses of each one.

The effectiveness of traceback methods based on hop-by-hop tracing may be limited by criminal adaptation and cross-border implementation challenges. Hop-by-hop tracing is easy to defeat on a technical level because criminals will find alternate routes for their traffic to prevent it being traced. They have decades of experience of routing international communications traffic to evade detection. Hop-by-hop tracing can also be obstructed by laws that prevent the international exchange of relevant data.

Even if all countries could be persuaded to support a global hop-by-hop method of tracing dialled voice calls, it would still be rendered redundant before it entered service because criminals would stop using dialled voice calls and start using other ways to transmit their voice. Phone users are switching to over the top services that allow them to speak and send messages to friends, family and businesses without dialling telephone numbers. So are scammers.

We should be clear about whether we want to speed up the way tracing has been done in the past – by making enquiries of each CP in turn – or if LEAs want to identify the sources of crime as directly as possible. Transmitting tracing and authentication data in-band within telecoms networks means it follows the same route as the communication, and hence incurs the risk of being interrupted at any hop. Transmitting data out of band avoids those risks because it only requires cooperation between the authorities and CPs at the origin and destination of the communication. Out of band methods are less mature at present but have a more realistic prospect of eventual success. Some individual nations are setting up out of band data exchanges between their telcos without trying to standardise for international cooperation. Meanwhile, the limitations identified in current STIR/SHAKEN implementations have prompted renewed interest in alternative approaches, including out of band SHAKEN and Open Verified Communication. The EU has an opportunity to become a technological leader in this domain by connecting the threads of this work to its eIDAS roadmap for digital ID.

European LEAs could look to the future by seeking general-purpose authentication and tracing systems that can also be applied to the newer generations of services that deliver voice and messaging communications through over-the-top and hybrid routes. This would involve out of band transfers of authentication and traceback data so the flow of data is independent of the specifics of the communication protocols implemented by the private sector. The benefit would be that a future-proofed tracing and authentication framework would ignore the increasingly artificial distinction between a voice call instigated using a dialled number or an app, or between text messages sent via SMS, RCS, WhatsApp and iMessage.

For all the focus on novel network technologies, it is easy to overlook the fact that Europe is already a world leader in tackling spoofing. The widespread adoption of ECC Recommendation (23)03 has greatly reduced the number of inbound international calls that spoof the domestic phone numbers of Europeans. Where figures are available, it is not unusual to see this control being credited for reductions in scam calls of around 70 or 80 percent. Its effectiveness greatly alters the cost-benefit argument for other controls that require different countries to cooperate. Sender ID registries are similarly effective at reducing the most common text message scams.

Some of the most effective anti-scam methods covered by this report have been put into effect in countries that have advanced anti-scam policies, such as Singapore and Australia. But Europe does not need to look to other continents for leadership. Ireland provides an example of a national strategy that has combined relatively simple measures with reported reductions in telecom-related scams.

The EU is well-placed to coordinate efforts to tackle networked crime, just as it led the telecoms and tech industries through the adoption of the GSM standards for mobile telephony, the introduction of mobile roaming, and the data privacy rules enshrined in GDPR. ECC Recommendation (23)03 is an example of recent European leadership in consumer protection; eIDAS establishes a positive future for digital ID that serves the needs of EU citizens. By first concentrating on methods that obstruct the flow of scam communications, and then implementing bilateral exchanges of data with countries that want to aid the prosecution of criminals they harbour, Europe can make the most tangible gains in reducing scams. Europe can do this by favouring the authentication and tracing technologies that already prioritise the goal of consumer protection while respecting European standards for security and privacy.

METHODS REVIEWED FOR THIS REPORT

Table 1: Methods Reviewed for This Report

Method	Is this method listed in the One Consortium tools inventory?	Does this method facilitate traceback?	Does this method reduce spoofing?
Blocking inbound international calls that spoof a domestic phone number; ECC Recommendation (23)03	No	No	Yes
SMS Sender ID registries and other registries based on the originating address of an A2P text message	No	Yes	Yes
Blocking of calls that spoof a phone number on a national do-not-originate list	Yes	No	Yes
Blocking of calls that spoof an invalid, unallocated or unassigned phone number	Yes	No	Yes
STIR, SHAKEN, RCD and VESPER	Yes	Yes	Yes
Out of band SHAKEN	No	Yes	Yes
Origem Verificada	No	Yes	Yes
Oculus 2FN (previously known as GSMA Call Check)	No	Yes	Yes
CHAKEN	No	Yes	Yes
AB Handshake	Yes	Yes	Yes
OVC	No	Yes	Yes
CIV	No	Yes	Yes
CodeB Sovereign SBC	Yes	Yes	Yes
ITU-T Q.3063	Yes	Yes	Yes
Heksagon Call Verification Services	No	Yes	Yes

SUMMARY OF EVALUATION SCORES FOR EACH METHOD

Table 2: Summary of Evaluation Scores for Each Method

Method	Proven Effectiveness	Range of Communication Channels	Range of Uses	Market Readiness	Anticipated Cost	Overall Score
Blocking inbound international calls that spoof a domestic phone number; ECC Recommendation (23)03	10	2	1	9	10	32
SMS Sender ID registries and other registries based on the originating address of an A2P text message	9	2	2	9	8	30
Blocking of calls that spoof a phone number on a national do-not-originate list	10	1	1	9	9	30
Blocking of calls that spoof an invalid, unallocated or unassigned phone number	7	2	4	7	9	29
STIR, SHAKEN, RCD and VESPER	5	2	8	9	0	24
Out of band SHAKEN	4	6	7	7	5	29
Origem Verificada	9	1	1	10	8	29
Oculus 2FN (previously known as GSMA Call Check)	4	10	10	2	9	35
CHAKEN	1	3	7	1	0	12
AB Handshake	3	5	5	3	10	26
OVC	4	5	5	3	10	27
CIV	3	2	2	2	10	19
CodeB Sovereign SBC	Not enough information to give a fair evaluation					
ITU-T Q.3063	Not relevant to deciding the future of call authentication in the EU					
Heksagon Call Verification Services	Outside the scope of this review					

1 - INTRODUCTION

10

WHAT IS SPOOFING, WHAT IS TRACEBACK, AND WHY ARE THEY LINKED?

Crime committed using electronic communications networks often involves impersonation. Criminals take advantage of the distance between them and their victim so they can more easily pretend to be somebody different to who they really are, or to represent something else than they really do. A scammer may claim to be a police officer who has telephoned their victim to warn them about an imminent crime; during the call they persuade the victim to transfer money into an account controlled by the scammer. A crime syndicate may send thousands of messages that appear to be from a legitimate delivery business to lure victims into clicking through to authentic-looking websites that collect credit card details as the supposed fee for delivering a package. An email that appears to come from an established supplier to a business has a bogus invoice attached, directing the company to make payment to a different bank account than before. In its most general sense, spoofing is a way to increase the chances that a victim will fall for the deception because the communication appears to come from an address that has been manipulated to appear authentic.

Various kinds of addresses are used in electronic communication. For example, an address could be a telephone number displayed as the origin of an incoming phone call or a series of alphanumeric characters presented in the 'sender' field of a text message. Spoofers may copy an address associated with a government institution, a well-known business or an individual human being.

Care is needed when using the word 'spoofing' because it can have a more precise definition in the context of a specific communication channel. For example, when a voice call is transmitted over a Public Switched Telephone Network (PSTN), spoofing refers to the practice of showing the recipient a phone number that is different to the phone number assigned to the device that actually originated the call. The phone number displayed on the recipient's handset is properly known as the Calling Line Identifier or Calling Line Identity (CLI), also known more casually as the 'caller ID'. There are both legitimate and illegitimate reasons to spoof a CLI, though businesses often object to the use of the word 'spoofing' when they make a legitimate substitution of a CLI. An example of a legitimate substitution would be a business making an outbound call to a customer that presents a general telephone number associated with that business, not the number specifically linked to the actual call centre agent who dialled the customer. This often occurs when the customer is located in one country and the call centre is located in a different country but the business would like their call to appear domestic in origin. Examples of illegitimate spoofing include call centres pretending to make sales on behalf of a business by displaying a CLI associated with that business although they have no relationship with that business.

The word 'spoofing' can also be used to describe analogous deceptions that involve written communications. The best-known example relates to email, whose core protocols allow relatively easy manipulation of the contents of the 'from' field within a message. The spoofing of email addresses became so widespread that internet businesses subsequently devised a number of countermeasures to highlight when email spoofing occurs, though software to discriminate between genuine and 'junk' email has never given results that are 100% reliable. A similar substitution of the originating address can occur in the context of other written electronic messages that are typically sent and received by phones, such as SMS. However, unlike email, the kinds of spoofing that can occur in text-based phone messages will depend on the specific details of how messaging systems have been implemented in each country. For example, European countries generally permit corporate entities who send SMS messages in bulk to present an SMS Sender ID as the origin address for their messages instead of presenting a mobile phone number. The SMS Sender ID comprises a string of letters and numbers. Each country will have different restrictions on the words and labels that can be presented as a Sender ID. Profane words may be banned, as may labels which are not specific enough, such as 'Alert' or 'Bank', because these are liable to abuse by bad actors. Even so, there may not be a national mechanism to prevent a label associated with one organisation being used by different organisations. And even in countries that do not enable alphanumeric SMS Sender IDs, there may still be spoofing of the telephone numbers presented as the origin of an SMS message.

A key difficulty with accurately describing all the forms of spoofing is that the best-understood examples belong in the past while criminals look to the future. Electronic communications networks are currently undergoing profound change. For example, numerous countries have set deadlines for 'switching off' their PSTN networks. In these countries, voice calls to dialled numbers will be carried over Internet Protocol (IP) networks from end-to-end, much like Voice over IP (VoIP) was popularised by Skype and has been incorporated into many proprietary communication protocols like those used for Microsoft Teams or WhatsApp. The differences between these voice services increasingly relate to the interfaces that users interact with, not to the network infrastructure that conveys the customer's voice. Put simply, the same voice can be conveyed by a wide variety of differently formatted streams of data, but each stream of data might still be carried along the same physical pipeline and the voice would still sound the same to the listener.

Another example of the current transformation of the communications sector relates to the severe decline of SMS as it is forced to compete with newer messaging protocols, including over the top services. Conventions for talking about communication are changing too. When somebody says they 'WhatsApped' their friend, do they mean that they spoke to them, messaged them, or both? Users of other services like Discord and Slack have their own unique terminology to describe the more evolved way in which communication occurs on those platforms, such as multiple users joining a single Discord 'server' to talk and message each other simultaneously, or Slack users speaking to each other via an instant 'huddle' that sits 'inside' of a text channel.

Systems to trace communications and prevent spoofing need to reflect the reality of the various back-end system protocols to be effective although phone users will not appreciate all the differences between technological protocols when they use communication services that appear to be similar from the user's perspective. Criminals are also indifferent to the back-end protocols they exploit; they only care about finding channels where the controls are not strong enough to disrupt their communications.



An ordinary phone user may just think of themselves as receiving a voice call or a text message without knowing anything of the increasingly complex, varied and hybrid channels used to convey those communications. For example, a person may receive an SMS message on their phone without knowing it had to be converted to the SMS protocol from the RCS Business Messaging (RBM) protocol used at the origin because of an inconsistency between some of the networks that carried the message from beginning to end. The same person may then receive an iMessage on their iPhone and will read it using the same app they also use to read SMS and RCS messages, without appreciating the differences between SMS, RCS and iMessage. These differences will matter to the police, as a system that can trace an SMS message may not be able to trace an iMessage. The police will then be confronted by limitations in the crimes they investigate which may appear arbitrary to the public.

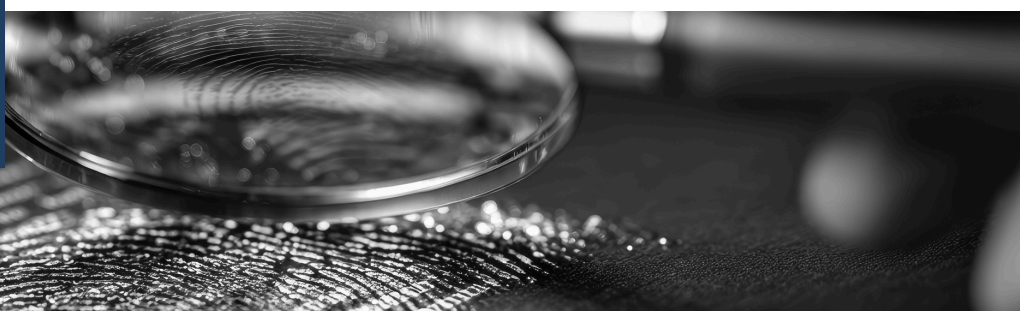
Similar hybrid issues can also arise with voice communications. For example, a phone user may receive a voice call through an app that runs on their phone without realising it began with somebody dialling their number on a circuit-switched PSTN network. If we only understand the word ‘spoofing’ by thinking of specific end-to-end technological, legal or regulatory contexts for how sounds or text may be conveyed, then we will fail to address the growing majority of hybrid scenarios that criminals will exploit. Or to put it another way, if we try to stop spoofing by implementing a technology that only works if one specific communications protocol is used from end-to-end, then criminals will easily defeat these technologies by choosing to speak and send messages to their targets using network routes that involve other protocols or a hybrid of protocols. The problem of how to deal with multiple protocols is especially severe for international communications because no national authority will be able to dictate that the same underlying protocols be used by all the communications providers involved in conveying the communication. The interoperability of communication services does not require absolute consistency in the use of the protocols and other technologies that deliver those services.

One key difficulty is that laws may not have kept pace with how people have changed their behaviours in practice. For example, a business and its customers may not think twice about speaking to each other via WhatsApp. However, national institutions that regulate CPs may have no authority over an Online Communication Service (OCS) like WhatsApp. The laws that address spam and scams in the context of a traditional dialled phone call may not have been amended to apply similar protections to users of OCS services. The best anti-scam work occurs when LEAs like the Singapore Police Force (SPF) take a holistic approach to all forms of electronic communication.

Data from countries that are advanced in the tackling of scams demonstrates that criminals will migrate from a well-controlled communication channel to channels that can more easily be exploited. For example, data published by the SPF showed scams initiated by SMS have fallen over time, from 2,367 in 2021 to just 450 in 2025, but that scams initiated by OCS text messaging services have risen from 5,095 in 2021 to 9,355 in 2025 [1]. A crackdown by Indian authorities on the abuse of application-to-person (A2P) SMS saw the number of consumer complaints fall from an average of 38,790 per month during 2020 to 11,657 per month during 2023, but complaints about the abuse of person-to-person (P2P) SMS soared during the same period, from 34,116 per month during 2020 to 101,912 per month during 2023 [2]. To try to solve the problem of scams by tackling each communication channel separately and waiting to see how criminals will adapt may be insufficient to address the long-term evolution of scam activity.

[1] Summarised from SPF annual reports at <https://commsrisk.com/fraud-dashboard/#singaporeContactMethods>

[2] https://www.trai.gov.in/sites/default/files/2024-10/CP_28082024.pdf



There is a simple and general technological reason for why the prevention of spoofing is commonly associated with the ability to trace a communication from its destination back to its source. If additional data is transmitted alongside the content of the communication for the purpose of verifying who originated the communication, then this data also serves as a form of proof for where the communication came from. Such data would need to be supported by a robust series of know-your-customer (KYC) checks to ensure the contents of the data are trustworthy, but there are various technologies that can convey data about the originator of a communication with negligible risk of the data being corrupted or manipulated during transmission. If a technology, as supported by KYC controls, provides a 100% guarantee that an incoming communication originated with a particular individual or business, then it would become trivial to retain records to ‘trace’ the origin of communications authenticated using that technology. This report will analyse the pros and cons of the technologies developed for connecting and transmitting authentication data for electronic communications.

Some of the language being used in the opening chapter of this report is already cumbersome, so it is worth introducing some common telecoms industry terminology. Communications originate with the person or business that instigated the communication, and they terminate at the other end. The originator of a communication is commonly referred to as the A-party, and the recipient is the B-party. Spoofing disguises the A-party so they appear to be somebody else. When the police trace a communication, they begin with what has been received by the B-party and seek to identify who was the actual A-party. We might think of a communication going on a journey from A to B. This gives rise to the possibility of the communication following different routes that traverse different intermediate CPs and networks. When industry insiders talk about multiple communications, they often refer to it as traffic.

Authentication is a technical term that means, per the way a system works, that the identity presented by a user has been found to be consistent with the user’s identity. However, that does not mean the user’s identity is trustworthy. If I create an email address for “donalddrump@gmail.com”, then the authentication of messages sent from that address would confirm that I am the user with that email address, but it would not establish that I am the President of the USA or anyone else named Donald Trump. Authentication only establishes the truth of who sent a communication when used in combination with processes that verify the identity of a user before they gain access to a system. These verification processes are commonly referred to as know-your-customer (KYC) checks. Telecoms industry insiders also refer to many kinds of variants of the know-your theme, such as know-your-business (KYB) for business customers, know-your-traffic (KYT) for the flow of communication data received from multiple parties, know-your-upstream-provider (KYUP) for the telcos that have sent this traffic, and so on. For brevity, we will use KYC as synonymous with all the know-your checks that exist.

It should be noted how traceback, when it points to information that has been verified through robust KYC checks, is much more generally applicable to the fight against crime than the prevention of spoofing. Not all criminal communications are spoofed, but any communication could be traced if it is linked to data that conclusively shows who was the A-party. We will discuss later in this report the commercial reasons why traceback methods tend to be presented as a byproduct of anti-spoofing methods, instead of anti-spoofing methods being presented as a byproduct of traceback methods.



Legal powers to trace communications are often enshrined in legislation to tackle terrorism and organised crime. In general, a trace just involves an LEA querying a CP about a communication, the CP examining the data it retained about that communication, which may then point to an upstream CP who handled the communication before them, which leads to a repetition of this cycle until the chain of investigation has been completed by the CP that provided the service to the actual A-party. As leading American telecoms fraud expert Tom Walker observed in his response to our survey:

“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.”

So the concept of traceback is not new, although perceptions surrounding the need and purpose of traceback have changed dramatically in recent years. This is because:

- National mechanisms to trace communications do not deal with the growing volumes of criminal communications that originate abroad;
- The replacement of traditional PSTN networks with IP-based network technologies has made it much easier and cheaper for criminals to use international communications to hide their identity and evade justice while targeting victims in a foreign country; and
- The cost of automating the creation of voice and text communications has fallen, giving criminals the opportunity to originate far larger volumes of communication unless there are controls specifically designed to limit the bulk abuse of communications.

We will discuss later in the report how differing perceptions of the relative importance of each of these factors encourage different policing philosophies in China and the United States of America. The context in Europe is more complicated than in either of the superpowers currently trying to set the agenda for how global cooperation will enable the tracing of international communications. For now, it is sufficient to emphasise that the need for international traceback and the profile of illegal communications that will be traced are heavily influenced by two factors that vary greatly from country to country and which have nothing to do with technology.

Which languages are spoken by the residents of a country and the relative ease or difficulty for criminals based in other countries to obtain staff or automated systems that will be able to convincingly communicate in those languages. For example, Brazilian authorities face less of a challenge in protecting Brazilians from scam international voice calls because it is less likely that criminal operations in other countries will seek and obtain staff who can convincingly speak Brazilian dialects of Portuguese. In contrast, speakers of Mandarin Chinese can be found in many countries in large enough numbers that they will be targeted by messages written in Mandarin despite living in countries where Mandarin is not widely spoken.

Which kinds of communication are already considered legal and conventional in a country? For example, a Brazilian who is already habituated to receiving many telemarketing calls may be at greater risk of being deceived by a scammer impersonating a business than a European who lives in a country which has always prohibited categories of telemarketing calls that are legal and common in Brazil. A British citizen who receives a cold call about transferring their pension may immediately suspect it is from a scammer because even legitimate financial institutions are not allowed to make such calls. French citizens will find it even easier to identify scams following the August 2026 introduction of a ban on all unsolicited telemarketing calls.

Some nations have implemented data exchanges between CPs in their own country to reduce crime. For example, one of the respondents to the survey conducted for this report, a business called jtendo, is responsible for implementing the exchange of data so Polish CPs can positively verify if traffic came from another Polish CP. Data exchanges are also being implemented to check if traffic did not come from another telco in the country; mobile operators exchange data about the roaming status of customers so they can determine if an inbound international call is from a customer of another national CP who is roaming abroad or if that customer's number has been spoofed. There are too many different non-standardised national schemes for data exchange to sensibly review them all. The main inference is that data exchanges between CPs to authenticate communications and enhance traceability are not too difficult to implement if there is cooperation between all the CPs involved, as occurs when a national authority that encourage them to work together. In contrast, international cooperation is much more difficult for reasons that have nothing to do with technology.

ESTIMATES OF THE SCALE OF NETWORKED FRAUD

The most persuasive measures of the seriousness of networked fraud do not come from surveys that attempt to calculate the total value lost to fraud committed using electronic communications. They come from observations about the dramatic increase in the number of people working in scam compounds around the world. Workers in scam compounds will be engaged in speaking, messaging and videoconferencing with potential victims on a daily basis. Those victims will usually be in a different country to the scam compound. The worker in the scam compound may consider themselves to have a regular job like those in legitimate call centres, except that they know their objective is to deceive the targets they communicate with. Or they might have effectively been enslaved by being forcibly trafficked or lured into moving to a foreign country by promises of a well-paid job, only to find their passport has been confiscated by their supposed employer and that armed guards prevent them from leaving the compound. There have been many documented cases of scam compound workers being violently beaten if they fail to meet targets for the amount they steal, and of the murder of workers who attempted to escape.

The following table summarises the best estimates of the number of scam compound workers in various countries.

Table 3 (cont.): Recent Estimates of the Number of Workers in Scam Compounds by Country

Country/ Region	Estimated Workers in Scam Compounds	Source(s)	Comments
Southeast Asia / Mekong region	At least 300,000	Office of the United Nations High Commissioner for Human Rights (OHCHR) [3]	A regional-wide estimate that overlaps with estimates for specific countries listed below.
Cambodia	100,000– 150,000	OHCHR [4] ; United Nations in Cambodia [5]	OHCHR reported at least 100,000 people forcibly involved in online scams. A later United Nations analysis gave the wider range shown here.
Myanmar	At least 120,000	OHCHR [6]	OHCHR provides this lower-bound estimate for people who may be held in forced scam work in Myanmar.
Laos	85,000	United States Institute of Peace (USIP) [7]	USIP described this as a conservative estimate of people working in Laos' scam industry.
India	More than 50,000	Investigation by Mark Rober, Jim Browning and Trilogy Media, reported by The New Indian Express [8] ; police estimates in Kolkata, Delhi and Mumbai [9][10][11]	The investigators reported access to a Telegram group containing more than 50,000 people described as employed by scam call centres across India. This total may include inactive or non-calling participants. However, the scale is consistent with police statistics for specific regions: 15,000 workers in Kolkata, more than 1,000 operational centres in Delhi, and around 2,500 centres between Malad and Borivali in Mumbai.
China	30,000	USIP [12]	USIP's regional comparison estimated approximately 30,000 people working in scam operations in mainland China.

[3] <https://searchlibrary.ohchr.org/nanna/record/35246/files/report-a-wicked-problem.pdf>

[4] <https://bangkok.ohchr.org/sites/default/files/documents/2025-01/online-scam-operations-2582023.pdf>

[5] https://cambodia.un.org/sites/default/files/2026-06/Cambodia%20Development%20Horizon%20Scan_final.pdf

[6] <https://bangkok.ohchr.org/sites/default/files/documents/2025-01/online-scam-operations-2582023.pdf>

[7] https://humantraffickingsearch.org/wp-content/uploads/2024/05/ssg_transnational-crime-southeast-asia.pdf

[8] <https://www.newindianexpress.com/india/2022/May/10/kolkata-epicentre-of-usd-20-billion-call-centre-scam-video-by-youtube-sleuths-goes-viral-2452005.html>

[9] <https://www.telegraphindia.com/culture/move-over-jamtara-tune-in-to-the-mysterious-and-evolving-world-of-scammers-and-cyber-fraud/cid/1897785>

[10] <https://indianexpress.com/article/cities/delhi/when-trouble-calls-behind-delhis-call-centre-scam-duping-us-citizens-7520358/>

[11] <https://www.hindustantimes.com/cities/mumbai-news/fake-call-centre-busted-in-borivali-101670958705685.html>

[12] https://humantraffickingsearch.org/wp-content/uploads/2024/05/ssg_transnational-crime-southeast-asia.pdf

Table 3 (cont.): Recent Estimates of the Number of Workers in Scam Compounds by Country

Country/ Region	Estimated Workers in Scam Compounds	Source(s)	Comments
Dubai	20,000	USIP [13]	USIP's regional comparison estimated approximately 20,000 workers in Dubai scam operations.
Pakistan	16,200– 21,600 implied across 54 raided centres	Pakistan Senate Standing Committee [14] ; National Cyber Crime Investigation Agency (NCCIA) [15]	This is the arithmetic result of multiplying 54 scam compounds raised by the authorities by an average of 300–400 workers that NCCIA said were typically employed in each one. A subsequent briefing said the exact number of compounds that remain could not be ascertained.
Philippines	11,000– 15,000	Presidential Anti- Organized Crime Commission (PAOCC) [16] , United States Institute of Peace [17]	The February 2025 estimate from PAOCC concerned illegal workers said to be conducting scamming activities after the introduction of the ban on offshore gaming operations. USIP's 2024 regional comparison estimated approximately 15,000 people working in scam operations in the Philippines.

These figures demonstrate the scale of the criminal enterprises that use communication services to defraud victims. But how should national law enforcement agencies relate these facts to the risk of somebody being scammed in the specific countries they each protect? It is typical when writing a report of this nature to begin with reliable estimates of the value of the crime to be addressed. That means this report should consider two categories of estimate.

- The value of crime that is committed using spoofing, as would be addressed by anti-spoofing systems; and
- The value of all crime committed using communication networks, irrespective of whether spoofing has occurred, because all such crimes could be addressed by tracing those communications.

Crime involving the spoofing of communications is evidently a subset of all the crime conducted using communication networks.

Estimates of the value of crime serve a dual purpose:

- They motivate an appropriate level of investment into reducing the crime; and
- They indicate the author has relevant expertise and is familiar with the best research available.

[13] https://humantraffickingsearch.org/wp-content/uploads/2024/05/ssg_transnational-crime-southeast-asia.pdf

[14] <https://www.senate.gov.pk/com/pressreleasedetail.php?id=MzE5&pressid=NjE5OA%3D%3D>

[15] https://www.senate.gov.pk/en/news_content.php?id=Njg2Nw%3D%3D

[16] <https://www.gmanetwork.com/news/topstories/nation/936377/paocc-we-ll-finish-illegal-pogo-ops-in-ph-within-a-year/story/>

[17] https://humantraffickingsearch.org/wp-content/uploads/2024/05/ssg_transnational-crime-southeast-asia.pdf

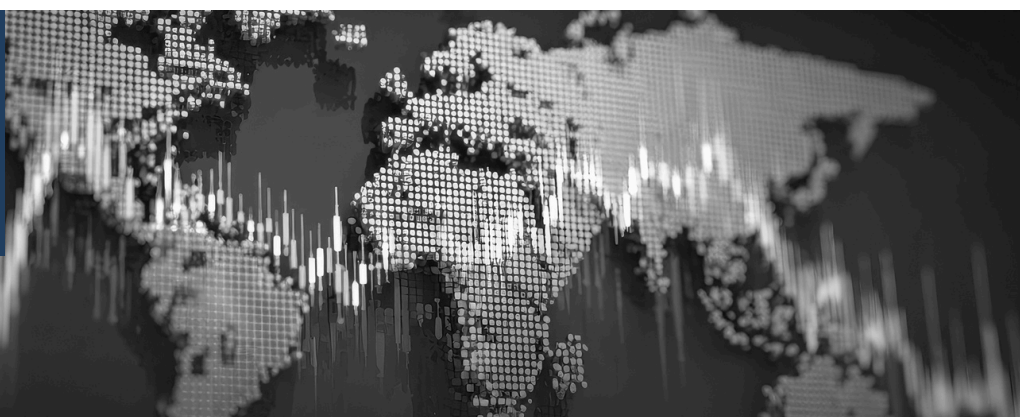
However, presenting quantitative measures of the crime committed using electronic networks is problematic because of the lack of reliable estimates and the extent to which estimates disagree with each other. An estimate from one credible source may be 10 times larger than an estimate from a different credible source. Estimates may swing wildly from one year to the next.

Some examples of differing estimates will be given below. The methods used to generate these estimates each have weaknesses that make them impossible to reconcile. They all agree in the sense that they all indicate that networked fraud is very large, and they all suggest that the amount spent by societies on mitigating networked fraud has been too small relative to the impact on victims and the amount spent on mitigating other crimes. They disagree in the totals presented and in the kinds of crimes included in those totals. Some of the most common issues with generating reliable estimates are:

- Underreporting of crime by the public;
- Overreporting of scam activity because communications that are not scams are mistaken for scams;
- Inconsistent categorisation of communication channels, such as one survey respondent including scams initiated by email in their figures relating to cybercrime, while another excludes them;
- Inconsistent categorisation of illegal activity, such as one survey respondent estimating only the losses caused by scams while another includes losses caused by other communications that are illegal but not scams (for example, because they are unsolicited communications which the recipient has not consented to receive); and
- Inconsistent categorisation of the value of losses ascribed to a particular communication channel because the scam involved multiple communications channels.

Consider a scenario where a phone user receives an SMS encouraging them to visit a website where they can download a fake app, and the app installed on the user's device then presents a warning that tells them to call a bogus helpline. We have no systematic way of accounting for how much of the victim's losses are due to the abuse of traditional telecom services (the SMS received by the victim, and the outbound voice call they made) and how much is due to the abuse of other cyber services (the fake website and the malware in the app that was downloaded). This can then lead to lots of unproductive arguments about how much of the blame for scams rests with social media companies, website hosting companies, domain name registrars, phone companies, etc.

The impossibility of reconciling estimates is exacerbated by studied ambiguity in the definitions of some of the most widely-reported estimates. It is common to see commentary that says 'most' of an estimated fraud loss involves the use of a telephone or spoofing, but without any precise breakdown of the figures. The lack of precision in defining what is included in an estimate may leave law enforcement ill-equipped to set the priorities for how they deploy their finite resources.



Many questions may be asked when deciding how to set policing priorities in a democratic society; these also get more complicated as societies adopt multiple new ways of communicating with each other, and hence new potential channels for committing crime. Our sense of priorities should influence how we evaluate the suitability of different kinds of methods that might be adopted to tackle crime, as each method will have differing strengths and weaknesses. The following paragraphs illustrate some of the relative priorities that need to be weighed when judging how well a method matches the ideal for tackling the networked crimes we most care about reducing.

Should the police focus on measures of the common consumer scams that cause the greatest losses to individual members of the public, or should they concentrate on measures of the potential liabilities of major institutions, such as banks, that may be forced to cover those losses? The answer to this question may seem obvious to some, but large corporate entities produce more reliable estimates of their own losses than surveys of the public. Big businesses can hence exercise greater sway over policing, even if they are not the primary victim of crime. Is it appropriate to determine priorities based solely on the absolute financial impact, or should other factors influence the level of effort devoted to tackling crime? Sexual abuse or cyberbullying may involve impersonation and they can be committed at a distance using networks but they may have no monetary impact on the victim.

Even if we only consider financial losses, police priorities may be influenced by the relative impact on different types of victims instead of the absolute amount stolen. For example, figures reported by the US Federal Bureau of Investigation (FBI) for 2024 showed that phishing and spoofing prompted approximately 200 times as many criminal complaints as SIM swapping, a different kind of telecoms fraud, but that the collective losses incurred by victims of phishing and spoofing were only three times greater than the collective losses of victims of fraudulent SIM swaps [18]. This is because SIM swap fraudsters will precisely target rich individuals with substantial cryptocurrency holdings. Much of the pioneering work done by a leading US law enforcement division in the realm of tracing electronic communications, the Santa Clara Rapid Enforcement Allied Computer Team (REACT) Task Force, stemmed from the criminal use of SIM swaps as a gateway to executing unauthorised transfers from the cryptocurrency wallets of Silicon Valley investors and executives.

The FBI figures also illustrate the volatility of reported fraud losses when drilling into more granular detail. The number of crimes categorised as phishing/spoofing was largely unchanged last year, falling from 193,407 in 2024 to 191,561 in 2025 [19]. There was also very little change in the number of crimes categorised as SIM swaps, which went from 982 in 2024 to 971 in 2025. However, the collective value of phishing/spoofing losses rose from USD 70.0mn (EUR 59.9mn) to USD 215.8mn (EUR 184.5mn), while the value of SIM swap losses fell from USD 26.0mn (EUR 22.2mn) to USD 17.4mn (EUR 14.9mn) over the same period. Scammers are like gamblers; they spend a relatively consistent amount of money on each attempt to scam a victim, but the proceeds fluctuate. Those proceeds depend not just on how often the scammers succeed, but also on the amounts that victims are able to lose. The volatility of reported fraud losses can be misinterpreted as evidence of a meaningful trend by inexperienced audiences.

Deciding policing priorities lies beyond the remit of this report, which is an examination of methods for mitigating and investigating crime. But those priorities are an important consideration when deciding which methods have the ideal design and which methods are not as suited to addressing the actual priorities of law enforcement agencies. This consideration also lies beyond the remit and expertise of most technologists and business people who are asked to comment on how to stop spoofing and how to trace communications. They may know how to do certain things, but they lack the knowledge or status to decide what needs to be done and why it needs to be done.

[18] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[19] https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

In the absence of a strong statement of priorities, or of clear measures of the relative importance of different categories of crime, experts in other domains may give advice that is unwittingly influenced by their subjective impressions about the nature of crime, who is responsible for that crime and who are the victims of crime. Special care is needed in an international context because racism and other irrational prejudices may influence perceptions about who is to blame for crime. This report will seek to be mindful of the distinction between the purpose and the design of a system to encourage readers to avoid the mistake of allowing the designs of certain systems to dictate their opinion about which objectives need to be pursued. For instance, if it is believed that most criminal communications originate abroad, it would be advantageous to block criminal communications using systems that can effectively stop them at border, even if somebody else can propose a different kind of solution that is very effective at tracing international communications back to their foreign origin.

Now we get to the part of the report that most readers would expect to see right at the beginning. Here is a table showing some of the most commonly quoted estimates of the global scale of scams and other frauds conducted using communication networks, some of which is effected via spoofing and much of which could potentially be curtailed if tracebacks were more common. Whereas most authors seek to boost their credibility by only presenting statistics that are large and consistent with each other, this table is ordered to emphasise how the statistics are large and inconsistent with each other. This inconsistency should not be treated as a flaw in this report but as an indicator of a more general problem with the quality of information gathered about networked crime. We lack investment in systems to measure how bad networked crime is, never mind the systems needed to reduce networked crime.

Table 4: Commonly Quoted Estimates of Global Communications Network Fraud

Source	Method	Year	Value (EUR bn)	Comments
Global Anti-Scam Alliance (GASA) [20]	Survey of 58,329 members of the public in 43 countries and markets	2024	881	An overestimate for the purposes of this report because it covers many kinds of scam and many kinds of communication.
Global Anti-Scam Alliance (GASA) [21][22]	Survey of about 46,000 adults in 42 markets	2025	378	An overestimate for the purposes of this report because it covers many kinds of scam and many kinds of communication.
Nasdaq Verafin [23][24]	Proprietary data modelling, a survey of more than 500 financial-crime professionals and executive interviews	2026	53	An overestimate for the purposes of this report as it includes frauds that may not have been facilitated by phone services, but also a possible underestimate because it excludes some frauds that can be conducted using phone services.

[20] <https://gasa.org/knowledge-base/blog/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai>
[21] <https://gasa.org/knowledge-base/reports/global-state-of-scams-2025>
[22] <https://gasa.org/knowledge-base/blog/gasa-policy-agenda-2026>
[23] <https://ir.nasdaq.com/news-releases/news-release-details/nasdaq-vera-fin-report-finds-financial-crime-epidemic-reaching>
[24] <https://ir.nasdaq.com/node/110136/pdf>

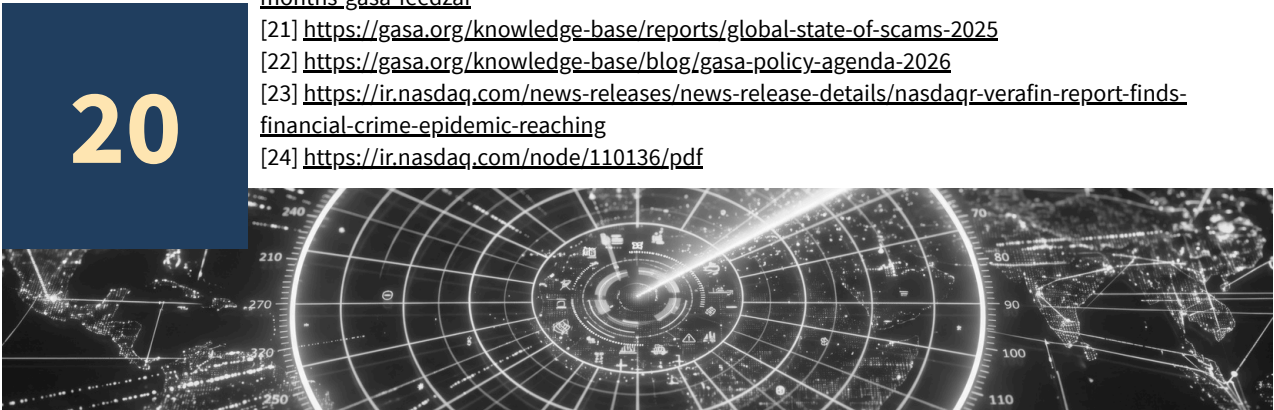


Table 4 (cont.): Commonly Quoted Estimates of Global Communications Network Fraud

Source	Method	Year	Value (EUR bn)	Comments
TransUnion [25] [26]	Survey of 1,200 business leaders in six countries	2025	442	The estimate is based on how much businesses reimburse consumer losses. However, the figure may exaggerate losses to consumers by including losses suffered directly by the business, without any consumer being victimised.
Communications Fraud Control Association (CFCA) [27]	Survey of approximately 50 telecoms professionals	2025	36	An underestimate for the purposes of this report because the bulk of the survey relates to frauds that victimise telcos, not frauds that victimise the public.

These figures relate to fraud, with each organisation asserting or implying that communication networks were used for most of the frauds included in their totals. The exact breakdown between frauds that depend on communication networks and frauds committed using other means is typically left vague. All of the estimates are heavily dependent on surveys, resulting in some ambiguity about the kinds of communications networks and channels used to commit these frauds. It is highly likely that crimes committed using modes of communication such as email, WhatsApp, iMessage, Microsoft Teams and direct messaging on social networks have been included in some of these estimates while others, such as the figure from the CFCA, will only relate to services supplied by traditional telephony providers.

The most noteworthy statistics come from GASA, not just because of the very large number and wide geographic spread of respondents to their survey, but also because of the dramatic fall in the value of reported fraud losses between 2024 and 2025. If the 57% decline in losses represented a genuine trend then fraud will soon be eliminated entirely! The likeliest explanation is that opinion polls exacerbate the underlying volatility of measures of fraud because they are also influenced by changes in who has been surveyed, their subjective state of mind, and recent events that may disproportionately affect their memory of what occurred over the previous 12 months.

Frauds that involve the spoofing of communications are necessarily a subset of all frauds involving communication networks. The lack of detail in estimates of networked crime makes it even harder to find reliable estimates of the losses due to spoofing. Estimates of the value lost to frauds that involve spoofing show there is general agreement that the problem is large but very little agreement on how large the problem is. Most figures estimate how much impersonation fraud has occurred in a country; spoofing aids impersonation, but impersonation can occur without spoofing. Per capita impersonation fraud losses are given in the following table to aid the comparison of figures from national sources.

[25] <https://newsroom.transunion.com/h2-2025-global-fraud-report/>

[26] <https://media.transunion.com/content/dam/transunion/za/business/collateral/report/3611950-h2-25-fraud-trends-rpr.pdf>

[27] <https://cfca.org/global-fraud-loss-survey-2025-report-published/>

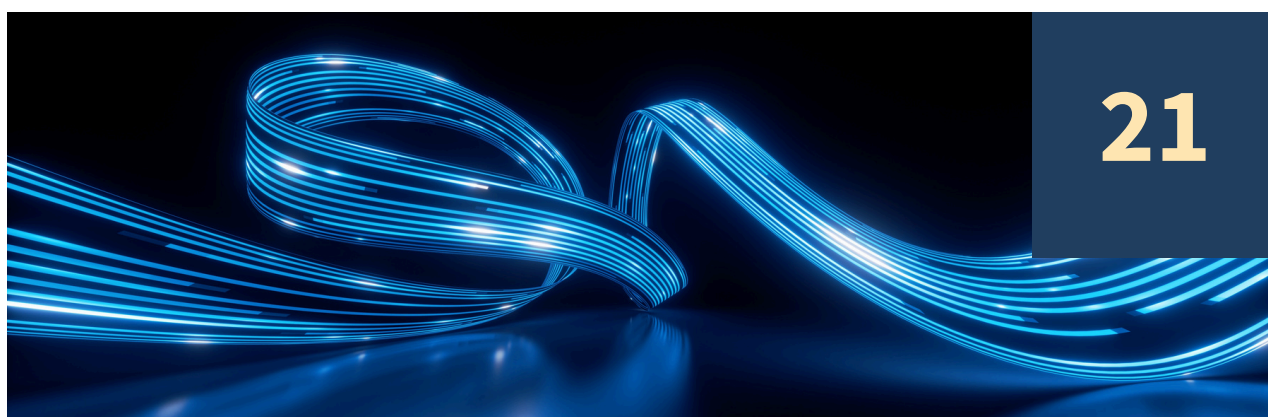


Table 5: Per Capita Impersonation Fraud Losses

Source	Method	Year	Total Loss (local currency)	Per Capita Loss (EUR)	Comments
Singapore Police Force [28]	Reported Government Official Impersonation Scam cases	2025	SGD 243mn	26.01	Includes calls and messages where the origin address was not spoofed
US Federal Trade Commission [29]	Complaints received from consumers	2025	USD 3.5bn	8.75	Includes imposter scams by telephone, text, email, social media, websites and online advertisements
Japan National Police Agency [30][31]	Police records of fake-police fraud	2025	JPY 101bn	4.67	Interim police data stated that 99.0% of initial contacts were made by telephone, but not how often the CLI was spoofed
UK Finance [32]	Reports from financial institutions	2025	GBP 92mn	1.5	Combines bank or police impersonation with other impersonation; these scams often begin with a phone call or text, but the total is not limited cases involving spoofing
Dutch Banking Association (NVB) [33][34]	Reports from member banks	2025	EUR 25.8 million	1.39	The figure relates to bank-helpdesk fraud, where criminals impersonate bank staff; it is not limited to cases involving a spoofed telephone number
Canadian Anti-Fraud Centre [35] [36]	Reports received from victims	2025	CAD 28.3 million	0.42	The category is classed as phone and fax and concerns criminals impersonating financial institutions, law enforcement and other trusted organisations; it is not limited to cases involving a spoofed phone number

[28] <https://www.police.gov.sg/-/media/SPF/Media-Room/Statistics/Annual-Scams-and-Cybercrime-Brief-2025/Annual-Scam-and-Cybercrime-Brief-2025.pdf>

[29] <https://www.ftc.gov/news-events/news/press-releases/2026/06/ftc-data-show-people-reported-losing-3-point-5-billion-imposter-scams-2025>

[30] <https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/260605/01.html>

[31] <https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/251202/01.html>

[32] <https://www.ukfinance.org.uk/system/files/2026-06/UK%20Finance%20Fraud%20Report%202026.pdf>

[33] <https://www.nvb.nl/nieuws/banken-roepen-socialmediaplatforms-op-meer-te-doen-aan-online-fraudebestrijding/>

[34] <https://www.nvb.nl/nieuws/banken-en-telecombedrijven-willen-wijziging-telecommunicatiewet-om-fraude-tegen-te-gaan/>

[35] <https://antifraudcentre-centreantifraude.ca/features-vedette/2026/02/month-prevention-mois-eng.htm>

[36] <https://antifraudcentre-centreantifraude.ca/scams-fraudes/b-investigateur-enqueteur-eng.htm>

There is strong evidence that there has been a significant reduction in the number of calls with spoofed CLIs received in some European countries during the last few years, and the same causal factors may also have reduced some of the losses cited above. This will be explained in more detail in the chapter on specific anti-spoofing methods and specifically in the section discussing international adoption of Recommendation (23)03 by the European Conference of Postal and Telecommunications Administrations.

Some fraud experts believe the contribution of spoofing to overall levels of fraud has been exaggerated to distract from a lack of enforcement of other consumer protection rules. This will be explored in more detail in the following chapter.

THE STRUCTURE OF THIS REPORT

Chapters 2 and 3 will elaborate on the questions that need to be asked of any international regime to tackle networked crime; we are unlikely to get the right answers if we do not ask the right questions. Chapter 2 will highlight the adaptability of criminals that exploit communications networks and how consumer protection and law enforcement efforts will need to be equally adaptable to keep pace with crime. Chapter 3 outlines the rival law enforcement philosophies of the two nations exerting most pressure for international coordination of the policing of communications, China and the USA, so we can put European options for tackling networked crime into a global context.

Chapter 4 briefly describes the approach taken to gathering information for subsequent chapters.

Chapter 5 provides a summary description of the work being done by the institutions that have the best chance of obtaining the international consensus required for effective international traceback. It should be noted that there is very little coordination of work between these institutions, to the point where they rarely acknowledge each other's work and may not even be aware of it. This complicates making a fair appraisal of who might ultimately provide international leadership and whose efforts will prove inconsequential.

Chapter 6 will evaluate each traceback and anti-spoofing method, with the final chapter making brief recommendations. This will be based on the principles articulated during this introduction, and in particular the assumptions made about the needs of law enforcement agencies operating in the EU. Other potential benefits, such as whether the solutions could also be used to generate new revenues from enhanced telemarketing, will not be considered.

All the information provided by survey respondents is presented in an [Annex available online](#).



INCLUSIONS AND EXCLUSIONS

It has been noted above that the word ‘spoofing’ can have several inconsistent meanings. Failure to differentiate between these meanings leads to confusion among non-expert audiences about the methods used by criminals and the ways of mitigating crime. They may then be disappointed to learn that there are kinds of crime not addressed by ‘anti-spoofing’ controls they previously believed to be comprehensive.

Clarity over the scope of an anti-crime control is vital for understanding the balance between the costs and benefits of that control, although vendors may emphasise the benefits of their solutions while devoting less attention to limitations and residual risks. The following paragraphs are written to provide precision over the kinds of spoofing and traceback that will be covered by this report, and the other forms of crime that are sometimes described with the word ‘spoofing’ but which are not addressed by the methods reviewed here.

The substance of this report covers the combination of tracing and anti-spoofing methods. The combination implies that the audience is interested in methods of tracing communications that involve multiple communications providers, not methods to trace a communication within a single provider or a single network. For example, the technical specifics of how to determine the location of a mobile phone when it sent an SMS message by tracing the message to a network base station are excluded.

Tighter controls over the sending of SMS messages in bulk have prompted criminals in many parts of the world to use portable radio devices commonly referred to as ‘SMS blasters’ to send messages directly to the mobile phones of victims without involving a genuine mobile network. There has been a significant acceleration in recent years in the rate of new reports of SMS blasters being used for crime in a much wider geographic spread of countries [37]. Making a direct connection with the phone using technology that operates like a network base station allows the criminal to bypass any alarms and filters implemented by network operators. As a consequence, their messages are also said to ‘spoof’ originating phone numbers and Sender IDs. However, there is no defence against this form of spoofing that can be implemented by CPs because they are not involved in the transmission of the communication at any stage. The relevant mitigations do not seek to stop the ‘spoofing’ of SMS blasters per se, but instead concentrate on locating the radio signal emitted by SMS blasters, arresting the criminals who operate them, and prohibiting the supply, import and ownership of SMS blasters without a legitimate reason. This particular form of spoofing is excluded from this report.

[37] <https://commsrisk.com/fraud-dashboard/#baseStationsSection> illustrates how known cases of SMS blasters being used for crime have spread to new countries over time



2 - HOW CRIMINALS ADAPT

25

The introduction to this report discussed some of the reasons it can be difficult to estimate the amount of crime conducted by criminals over the telephone. This section covers some of the reasons why generalisations about crime may be wrong. In particular, criminals change their methods so rapidly that generalisations about the current techniques favoured by criminals can be based on information that is already out of date.

The following graph illustrates the point about placing too much reliance on old assumptions. It compares complaints made by American consumers about unwanted calls with the value of the fraud losses they incurred because of a scam that began with a voice call. The drop in the line showing the number of complaints about unwanted calls received by the US Federal Trade Commission (FTC) has often been described as evidence of the effectiveness of the US anti-scam strategy. It has even been cited as proof of the effectiveness of the strategy during testimony to the US Congress [38]. However, a different picture is painted by the rising value of losses instigated by a phone call. Stopping high volumes of highly repetitive automated calls created by scammers does not mean scammers are not refining their techniques and finding better ways to reach victims. Note that the anomalous figures for the final quarter of 2025, highlighted in yellow, are due to the interruption in data collection caused by the temporary shutdown of the US government during that period, not due to an actual fall in scam activity.

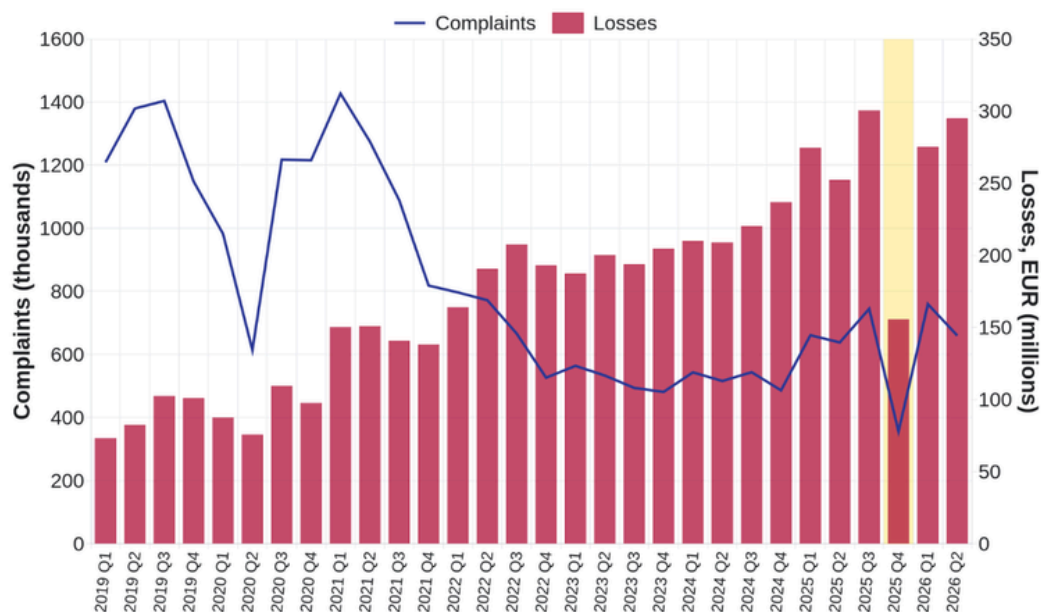


Figure 1: Quarterly Complaints about Calls vs Value of Scams Initiated by Call per FTC [39][40]

[38] <https://www.govinfo.gov/content/pkg/CHRG-119hhrg60677/html/CHRG-119hhrg60677.htm>

[39] <https://www.ftc.gov/policy-notice/open-government/data-sets/do-not-call-data>

[40] <https://public.tableau.com/views/FraudReports/ContactMethod>

It is a mistake to make simple inferences from the number of attempted scam communications to the amount that the public loses as a result of scam communications. The Australian authorities maintain more detailed statistics about the number of scam communications reported by the public and the value lost to scammers. The following graphs show that while the situation is improving in Australia, there is little correlation between the number of scam calls, the number of scam text messages, and the amounts being lost as a result of scams instigated by either kind of communication.



Figure 2: Quarterly Australian Scam Call Complaints vs Reported Losses [41][42]



Figure 3: Quarterly Australian Scam Text Complaints vs Reported Losses [43][44]

[41] <https://www.acma.gov.au/action-spam-and-telemarketing>
 [42] <https://www.scamwatch.gov.au/research-and-resources/scam-statistics>
 [43] <https://www.acma.gov.au/action-spam-and-telemarketing>
 [44] <https://www.scamwatch.gov.au/research-and-resources/scam-statistics>

Figures from Canada reinforce the same conclusion. Just because the total number of scam communications has fallen does not mean criminals are stealing less than before.

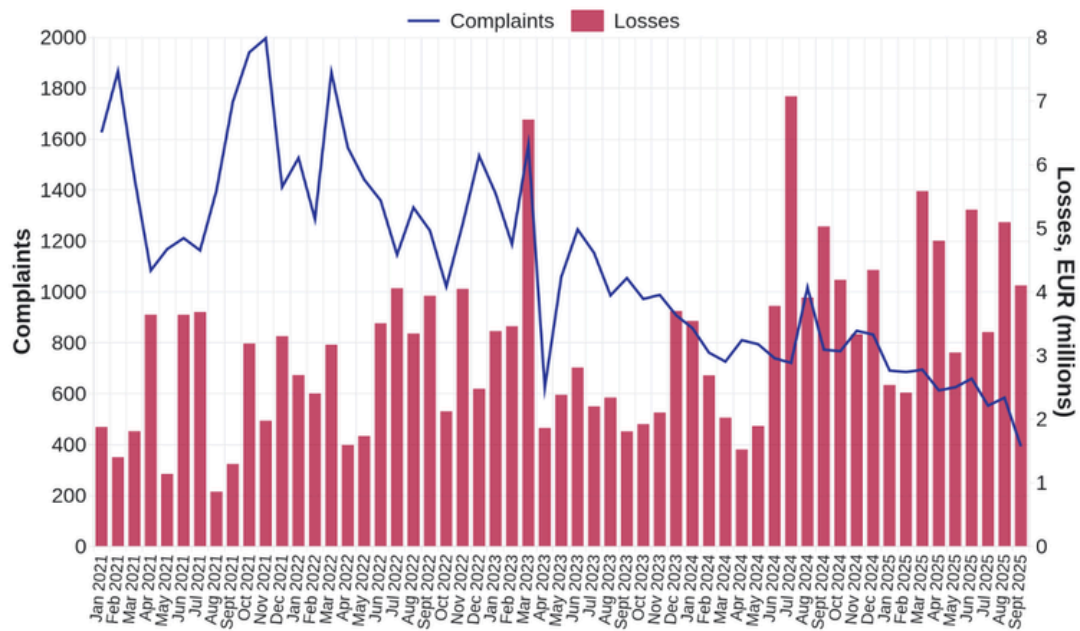


Figure 4: Monthly Canadian Fraud Complaints Involving Calls vs Reported Losses [45]

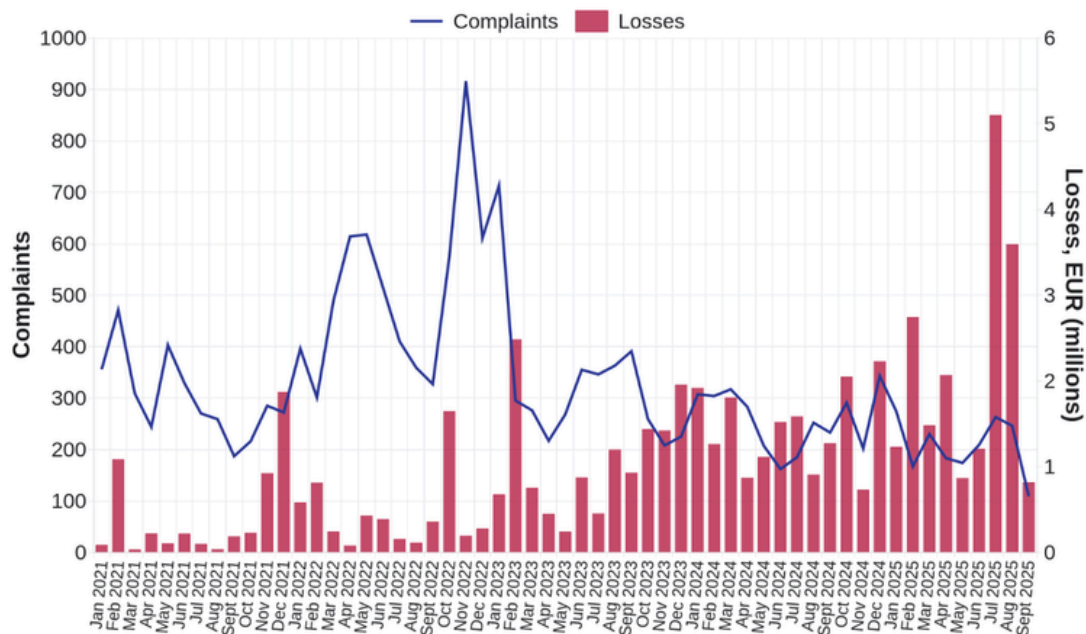


Figure 5: Monthly Canadian Fraud Complaints Involving Text Messages vs Reported Losses [46]

[45] <https://open.canada.ca/data/en/dataset/6a09c998-cddb-4a22-beff-4dca67ab892f>

[46] <https://open.canada.ca/data/en/dataset/6a09c998-cddb-4a22-beff-4dca67ab892f>



The complex relationships evidenced in these graphs suggest that many claims made about the effectiveness of anti-scam policies are based on inadequate data or inadequate analysis of the data. When enlisting the help of experts to analyse crime trends, LEAs should seek balance by also listening to experts with less favourable interpretations of the data than those provided by representatives of the telecoms sector. Some good examples of contrasting opinions were given in the responses to the survey run for this report. Tom Walker, a professional who spent 20 years working closely with the police while investigating fraud on behalf of T-Mobile USA and AT&T, highlighted the nature of criminal adaptation while challenging the motives for this research paper when he observed:

“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.”

I do not agree with Tom’s opinion that reducing spoofing does not reduce fraud. However, Tom’s opinion deserves respect because he has had access to relevant data that is not in the public domain. There is merit to his argument that the impact of technologies designed to reduce spoofing within the USA has been greatly exaggerated. One root of this exaggeration is that sophisticated criminals will rapidly change their approach while unsophisticated anti-fraud professionals continue to focus their efforts on older ways of detecting crime. As a consequence, the totality of crime can be underreported because only the older types of crime are being detected.

A related observation about the adaptability of fraudsters was made by Heksagon, a Serbian business with visibility of telecoms crimes because of the firewall systems they supply to CPs. When discussing methods to tackle scams instigated by a text message, they noted:

“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.”

The universal truth of this observation is illustrated by the trends in complaints statistics when India’s national authorities cracked down on scam and spam messages sent using application-to-person (A2P) SMS channels, only to see runaway abuse of person-to-person (P2P) SMS.

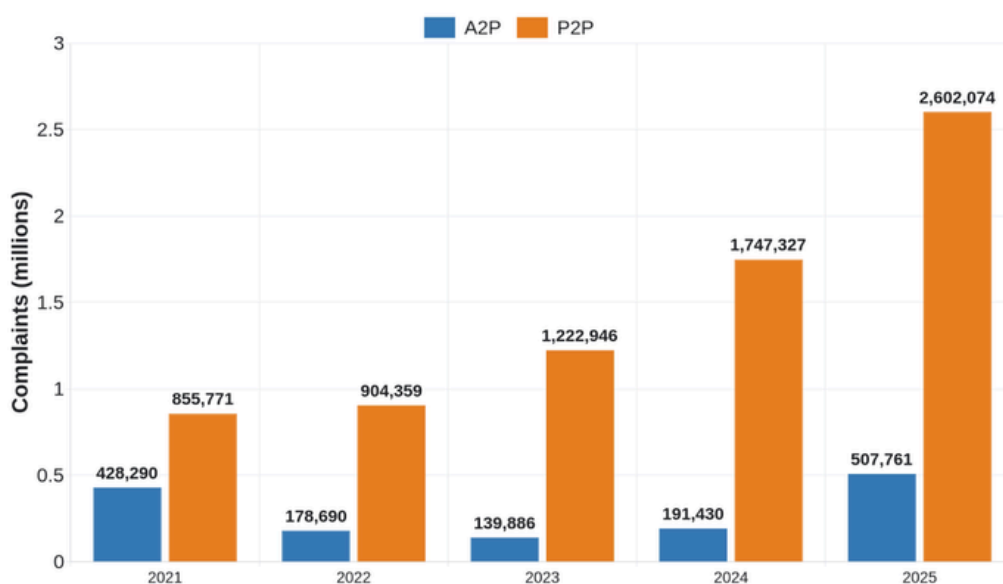


Figure 6: Complaints About Unwanted Commercial Communications via A2P and P2P in India [46][47][48]

[47] <https://www.trai.gov.in/notifications/press-release>

[48] <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2223950&=3&lang=2>

[49] https://sansad.in/getFile/rsnew/Committee_site/Committee_File/ReportFile/15/213/254_2025_10_16.pdf?source=rajyasabha

SCAMMERS ARE MOVING BEYOND TRADITIONAL TELEPHONY

Scammers do not just migrate from one service from a traditional telephony provider to another service from a traditional telephony provider. They also switch from traditional telephony services to OCS services supplied 'over the top' of the internet.

SINGAPORE

SPF data shows that scam cases initiated by SMS fell from 2,367 in 2021 to 450 in 2025, a decline of 81%. Frauds instigated by a dialled voice call have risen from 2,883 to 5,477 over the same period, though the figure has fallen for two consecutive years from a peak of 7,196 in 2023. Meanwhile, scam cases initiated through OTT messaging platforms rose from 5,095 to 9,355, and cases instigated by social media rose from 6,095 to 10,448. WhatsApp accounted for 54% of the cases involving OTT messaging. The available evidence suggests that all the benefits delivered by improved anti-scam controls over traditional telecoms services will not compensate for the overall increase in scams if online communications channels are not brought under control as well.

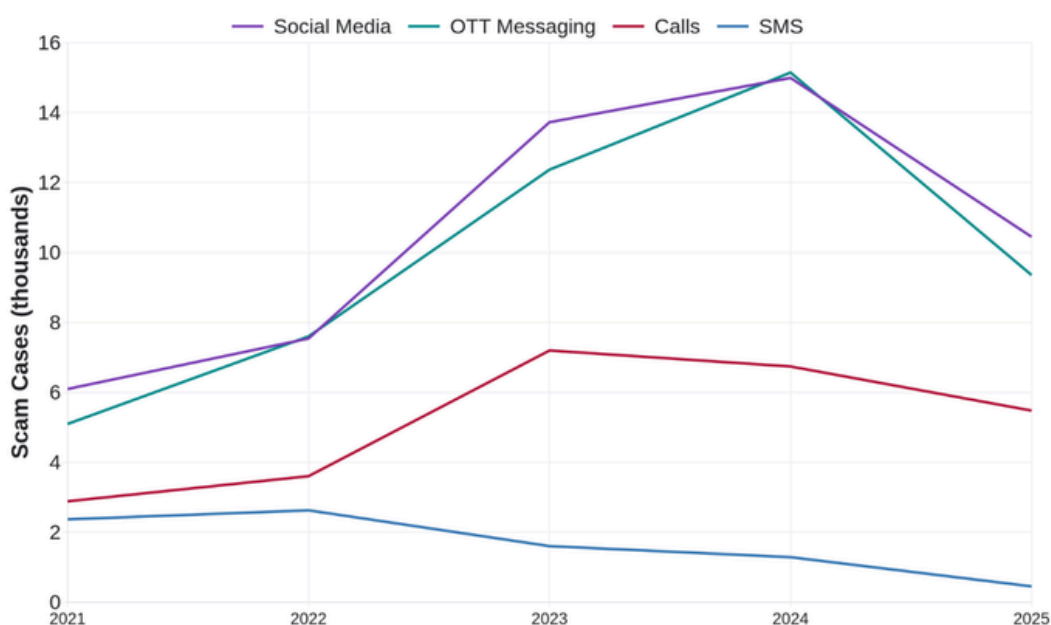
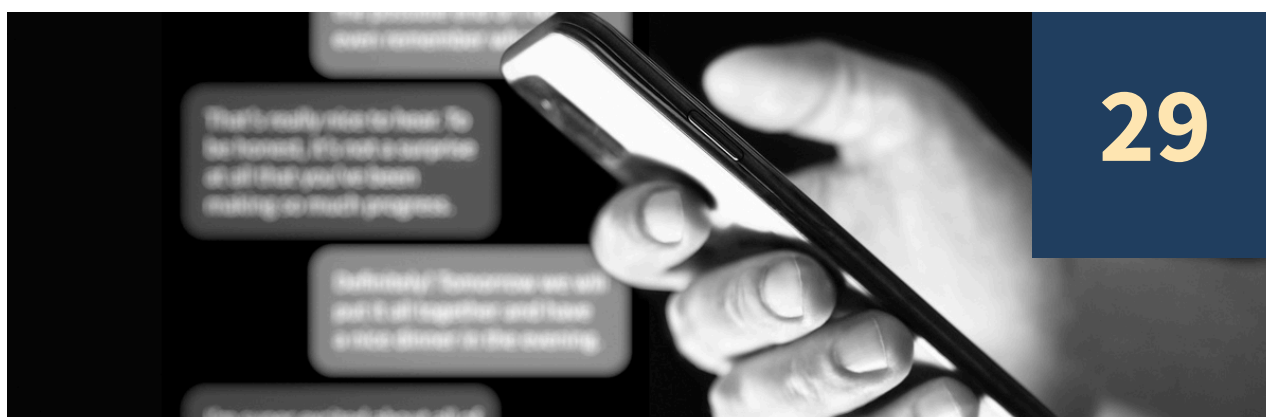


Figure 7: Annual Scam Cases by Initial Contact Method in Singapore [50]

CROATIA

Croatian Ministry of the Interior data shows that, for fraud offences, SMS/MMS was associated with 13 cases of fraud in 2021 and 35 in 2025, while cases involving OCS messaging and content-sharing applications rose from 15 to 131 during that time. For computer fraud, SMS/MMS rose from 5 to 13 during that period while scams instigated by OCS applications rose from 32 to 80.

[50] Singapore Police Force Annual Scams and Cybercrime Briefs, 2022–2025 <https://www.scamshield.gov.sg/archive/>



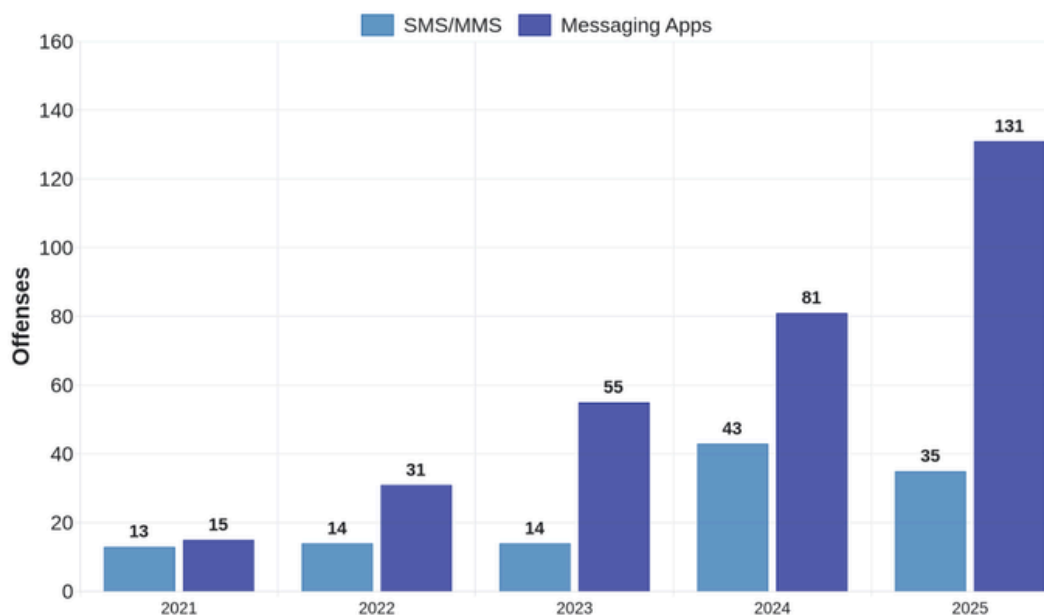


Figure 8: Police Statistics for Fraud Using SMS/MMS or Messaging Apps in Croatia [51]

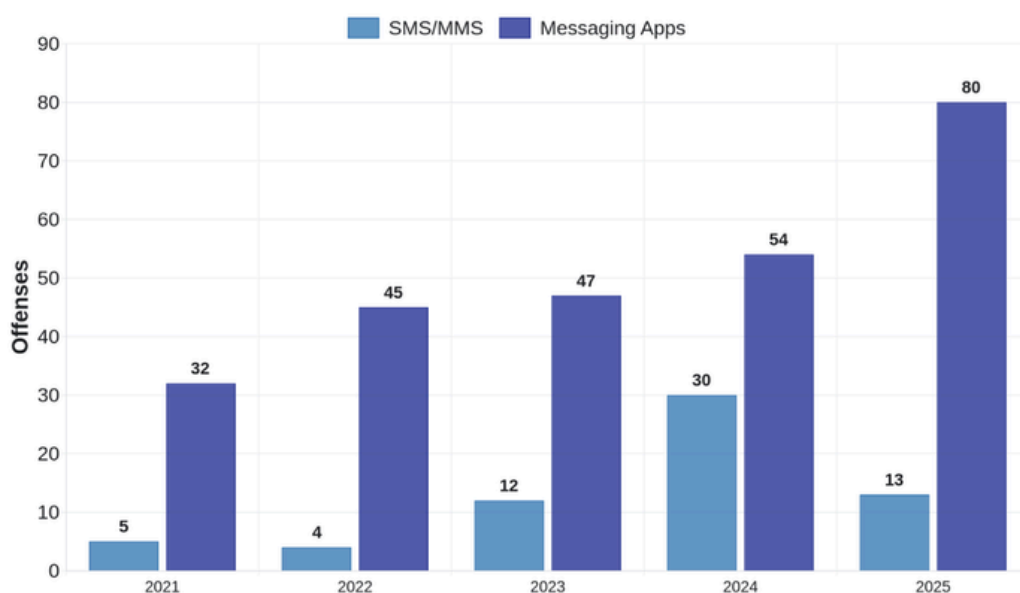


Figure 9: Police Statistics for Computer Fraud Using SMS/MMS or Messaging Apps in Croatia [52]

POLICING IN THE CONTEXT OF GLOBAL COMMUNICATION NETWORKS

Available evidence suggests that crime syndicates consciously establish scam call centres that target victims in other countries for two reasons:

- They prefer to base operations in jurisdictions where local law enforcement are less likely to intervene; and
- Solely targeting victims in foreign countries means there is less incentive for government or police to devote resources to finding and prosecuting the scammers based in their country.

[51] Croatian Ministry of the Interior, annual surveys and overviews of basic public-safety indicators, 2021-2025, <https://mup.gov.hr/statistics-121/121>

[52] Croatian Ministry of the Interior, annual surveys and overviews of basic public-safety indicators, 2021-2025, <https://mup.gov.hr/statistics-121/121>

The falling cost of international communications, especially when carried over the internet, and the increasing availability of newer technologies which enable good network connections in remote regions, such as satellite broadband, have made it feasible for criminals to behave like multinational corporations when deciding where to site their operations. They can choose countries and regions where staff and other operating costs are low, and where the risk of intervention by law enforcement is also low. This is reflected in the number of scam call centres established in war zones where government authority has been disrupted, and human trafficking is rife, such as regions of Myanmar that border China, or in districts of cities where there is a ready supply of potential staff and the office space for seemingly legitimate call centres can be obtained relatively cheaply, such as Gurugram.

Scams may be operated from the same office floor as a legal business model that also targets customers in foreign countries. For example, Philippine law enforcement has conducted a series of raids in recent years against scam call centres that were originally established as Philippine Offshore Gaming Operators (POGOs), a licensed business activity that provided online gambling to customers in China, where gambling is illegal. POGOs were later made illegal following a change in the Philippine government, but the business model of hiring staff to persuade residents of mainland China to engage in illicit gambling was already suited to conducting scams as well.

The transfer of data involved in authenticating an international communication (to prevent spoofing) or to trace the origin of a communication gives rise to jurisdictional issues that may not be immediately apparent to either technologists or lawyers. Lawyers may not appreciate the idiosyncrasies of how communications can be routed through systems located in intermediate countries. Technologists may not be conversant with the legal implications of transmitting data through those countries. This leads to a common misperception that the data required to authenticate or trace a communication can be legally exchanged between the originating and destination countries so long as the transfer of data is considered legal in both of those countries. In fact, the legality of a data transfer can come into question in all of the intermediary countries as well, depending on the technology that is being used to transfer that data and the purpose for which the data is used.

The following example is an illustration of the issues that can arise in practice. For 30 consecutive months between 2015 and 2018, internet traffic between Los Angeles and Washington DC was routed through servers in mainland China [53]. The routing of domestic US internet traffic through China may have been accidental or deliberate. It occurred because China Telecom forwarded anomalous Border Gateway Protocol (BGP) instructions for how to route traffic destined for US telecoms carrier Verizon. Various international telecoms carriers routed traffic destined for Verizon per the anomalous BGP instruction, sending it to Verizon via China Telecom. The telcos that routed traffic through China included Sweden's Telia, India's Tata and the UK's Vodafone. As well as the surveillance risk that comes with the routing of traffic, there is also the risk that data will be stripped or blocked in transit. If the Chinese government chose to impose a general or specific prohibition on the transfer of certain kinds of data across Chinese-owned networks, then this would obstruct any authentication or traceback process dependent upon that data.

Even in the case of an investigation involving communication between two parties in the same country, jurisdictional issues can arise if the actual route for the transfer of data traverses another country. In practice, there is a great deal of variety in how communications between two countries may be routed through intermediate countries. Where the flow of data depends on common legal norms, the scammer only needs to identify and use one route through a non-compliant country to ensure none of their communications will be traced back to the origin. Law enforcement, in contrast, will need traceback systems to work smoothly across all possible routes between the A and B parties. This has significant implications for evaluating whether the technological design of an international traceback system can fulfil its intended purpose in practice.

[53] <https://arstechnica.com/information-technology/2018/11/strange-snafu-misroutes-domestic-us-internet-traffic-through-china-telecom/>



3 - RIVAL PHILOSOPHIES FOR POLICING GLOBAL NETWORKS: CHINA, THE USA, AND EUROPE

32

Evaluating traceback systems that are meant to work across borders without first reaching international agreement on how to police communication networks results in a conundrum. How can we determine if a traceback system will work in practice if we do not yet know which jurisdictions will allow the system to operate? Are there parts of the world where networks will not be able to support the traceback protocols implemented elsewhere, thus preventing a trace from being completed between those two regions? What technological design features, such as those relating to privacy and security, will be required to meet the expectations of jurisdictions that must consent to the operation of the traceback system if those jurisdictions have not yet expressed how much (or how little) privacy and security over the transfer of data they will demand? It would be naive to suggest that one country or one group of countries can simply implement a technology to trace communications and then assume all other countries will adopt both compatible technologies and the legal norms required for the traceback system to work unimpeded across borders.

To further understand the interactions between technology and law, it is worth examining two distinct national philosophies for law enforcement and how they relate to the tracing of international communications. China and the USA are the two largest economies in the world, are each home to some of the world's most important communications providers, and have each demonstrated over the course of several years their radically different philosophies for how to tackle networked crime. Each has sought to increase their influence over the ways that other countries operate communication networks, most notably expressed by the first Chinese Secretary-General of the United Nations' International Telecommunication Union (ITU), Houlin Zhao, being elected in October 2014, and that his successor was the second American to be elected Secretary-General, Doreen Bogdan-Martin, the current incumbent. These elections represent a genuine competition between rival philosophies for how the coordination of international networks will be governed, with implications for security, privacy and the more specific goals addressed by traceback and authentication systems.

THE PEOPLE'S REPUBLIC OF CHINA

Mainland China has the most phone users in the world [54] and is home to three of the five largest telcos in the world as measured by subscriber numbers: China Mobile, China Telecom and China Unicom. It is also home to leading global manufacturers of telecoms networks, with Huawei and ZTE remaining considerable rivals to Ericsson and Nokia in the supply of 5G networks despite the impact of US-led trade barriers. China's population is the target for a considerable amount of scam activity conducted by scam call centres located in other countries. The extent of cross-border scam activity is also apparent through scams in the Mandarin language being reported across Europe and in other countries with only a minority of Mandarin-speaking residents.

[54] <https://worldpopulationreview.com/country-rankings/cell-phones-by-country>.

In 2016, the Chinese government ramped up severe penalties for scammers who use communication networks [55]. They backed the new legislation with active police enforcement both within China and abroad. The Chinese government has consequently pursued a series of bilateral policing agreements to tackle networked scams, principally with countries around Southeast Asia, including those countries with the highest reported numbers of staff working in scam call centres. Chinese participation would likely be an important factor in the success of any global traceback strategy.

Despite the preponderance of technology experts and resources available to them, the Chinese law enforcement philosophy has emphasised more traditional methods of gathering intelligence over the introduction of novel technologies. Chinese police work with foreign law enforcement agencies to determine the physical location of scam compounds, then conduct raids resulting in the arrest and extradition of the people working within. Some of these raids result in the extradition of thousands of people at a time. Leaders of gangs that run scam compounds risk severe punishment, including the death penalty. Per our research, China has orchestrated extraditions from scam call centres operating in all of the following countries.

Country	No. of people	Date	Links
Armenia	129 people	7 Sep 2016	https://www.foxnews.com/world/armenia-sends-129-telecoms-fraud-suspects-to-china https://en.mofa.gov.tw/News_Content.aspx?n=1329&s=32742
Bangladesh	28 people	28 Dec 2018	https://www.xinhuanet.com/english/2018-12/28/c_137704604.htm
Cambodia	25 people	24 Jun 2016	https://www.moj.gov.tw/2832/2833/2834/2835/59146/post
Cambodia	74 people	6 Jul 2017	https://www.chinadaily.com.cn/china/2017-07/07/content_30022239.htm
Cambodia	122 people	24 Aug 2017	https://www.xinhuanet.com/english/2017-08/24/c_136552882.htm
Cambodia	74 people	12 Oct 2017	https://www.investing.com/news/world-news/cambodia-deports-74-chinese-arrested-for-telecom-extortion-scams-540424
Cambodia	89 people	11 Apr 2018	https://english.cambodiadaily.com/2018/04/12/cambodia-deports-89-suspects-online-scam-china/ https://www.foxnews.com/world/cambodia-deports-89-suspects-in-online-scam-to-china
Cambodia	91 people	15 Oct 2018	https://www.phnompenhpost.com/national/chinese-police-escort-deported-scam-suspects
Cambodia	233 people	6 Dec 2018	https://www.xinhuanet.com/english/2018-12/06/c_137655521.htm
Cambodia	142 people	25–28 Sep 2019	https://english.cambodiadaily.com/2019/10/01/cambodia-deports-142-chinese-for-telecoms-fraud/
Cambodia	130 people	13 Apr 2024	https://www.rfa.org/english/news/cambodia/online-scam-deportations-04152024144201.html https://en.people.cn/n3/2024/0413/c90000-20156486.html
Cambodia	more than 680 people	By 21 Apr 2024	https://english.news.cn/20241128/6a3129b8ea984739b171fca75cdfaf2c/c.html

[55] <https://commsrisk.com/china-cracks-down-on-telecoms-fraud/>

Country	No. of people	Date	Links
Cambodia	240 people	28 Nov 2024	https://english.news.cn/20241128/6a3129b8ea984739b171fca75cdfaf2c/c.html https://www.gmanetwork.com/news/topstories/world/928610/china-repatriates-240-online-gambling-fraud-suspects-from-cambodia/story/
Cambodia	nearly 190 people	13–14 Apr 2025	https://www.rfa.org/english/cambodia/2025/04/14/china-taiwan-cambodia-deportation/ https://www.straitstimes.com/asia/east-asia/cambodia-deports-unknown-number-of-taiwanese-to-china-on-fraud-charges-taiwan-says
Cambodia	3 people	6 Jan 2026	https://apnews.com/article/b32da55af90841d6b2b95cc6334f3fa7
Cambodia	312 people	8 Feb 2026	https://akp.gov.kh/post/detail/361617 https://english.cambodiadaily.com/2026/02/12/cambodia-deports-319-chinese-nationals-over-online-scam-allegations/
Cambodia	1 person	1 Apr 2026	https://apnews.com/article/d3bb4f2cacda45204b35cfc8ac3d3681
Cambodia	1 person	17 Jun 2026 announcem ent	https://english.news.cn/20260617/6bccde6060aa4c948844cc633fd30d6c/c.html
Croatia	61 people	18 Jan 2018	https://www.taipeitimes.com/News/taiwan/archives/2018/01/26/2003686456 https://www.xinhuanet.com/english/2018-01/30/c_136934882.htm
Czech Republic	8 people	9 Apr 2020	https://www.usoud.cz/en/current-affairs/judgment-ii-us-2299-19-diplomatic-assurances-and-risk-of-torture-or-other-ill-treatment-associated-with-the-extradition-to-the-peoples-republic-to-china https://praguemonitor.com/news/national/14/04/2020/2020-04-14-czech-court-bars-extradition-8-taiwanese-china/
Fiji	77 people	4 Aug 2017	https://www.fijivillage.com/news-feature/Chinese-nationals-involved-in-telecom-and-online-fraud-cases---Fiji-Police-kr2s95/ https://www.fijitimes.com.fj/fiji-and-china-no-extradition-treaty/
Indonesia	86 people	10 Nov 2015	https://en.antaranews.com/news/101386/indonesian-police-deports-86-chinese-nationals-involved-in-cybercrimes
Indonesia	143 people	4 Aug 2017	https://www.antaranews.com/berita/644723/143-pelaku-penipuan-di-indonesia-tiba-di-china



Country	No. of people	Date	Links
Indonesia	153 people	20 Sep 2023	https://inp.polri.go.id/artikel/chinese-love-scammers-deported-from-indonesia https://english.news.cn/20230921/02006a060fee430bb37f6800ac4b30a9/c.html
Indonesia	9 people	27 Oct 2024	https://www.antaranews.com/berita/4420449/imigrasi-perak-deportasi-komplotan-pelaku-penipuan-daring-asal-china https://inp.polri.go.id/artikel/tanjung-perak-immigration-deports-chinese-online-fraudsters
Kenya	77 people	8–13 Apr 2016	https://time.com/4293337/china-taiwan-kenya-deportation-fraud/
Kenya	40 people	By 10 Aug 2016	https://www.mfa.gov.cn/fyrbt_673021/dhdw_673027/201608/t20160810_5434333.shtml
Laos	470 people	30 Dec 2015 raids; 8 Jan 2016. announcement	https://en.people.cn/n3/2016/0108/c90882-9001269.html
Laos	104 people	12 Jan 2018	https://www.xinhuanet.com/english/2018-01/12/c_136891603.htm
Laos	164 people	11 Sep 2023	https://laotiantimes.com/2023/09/11/lao-police-hand-over-164-people-suspected-of-online-fraud-to-china-at-wattay-international-airport/ https://www.thestar.com.my/aseanplus/aseanplus-news/2023/09/11/lao-police-hand-over-164-people-suspected-of-online-fraud-to-china-at-wattay-international-airport
Laos	462 people	28 Nov 2023	https://laotiantimes.com/2023/12/06/joint-police-operation-takes-down-462-online-fraud-suspects-in-golden-triangle-sez/
Laos	268 people	Jan 2024; announced 28 Feb 2024	https://laotiantimes.com/2024/02/29/lao-chinese-authorities-team-up-to-bust-online-fraud-dens-arresting-268-suspects/ https://www.rfa.org/english/news/laos/repatriate-03042024165756.html/
Laos	250 people	23 Apr 2024 announcement	https://laotiantimes.com/2024/04/24/joint-effort-between-laos-china-results-in-major-bust-of-telecommunication-fraud-rings/
Laos	280 people	23 Jun 2024	https://www.vientianetimes.org.la/freefreenews/freecontent_125_Police_y24.php https://www.thestar.com.my/aseanplus/aseanplus-news/2024/07/02/police-deport-280-chinese-nationals-on-charges-of-telecom-fraud
Laos	108 people	Aug 2024	https://www.rfa.org/english/news/laos/golden-triangle-call-centers-raid-08212024154847.html https://thediplomat.com/2024/08/lao-chinese-officials-detain-771-in-raid-on-golden-triangle-gambling-hub/
Laos	494 people	22 May 2026 announcement	https://www.globaltimes.cn/page/202605/1361673.shtml
Laos	170 people	24 Jun 2026	https://laotiantimes.com/2026/06/25/laos-intensifies-scam-crackdown-nearly-900-arrested-since-early-june/

Country	No. of people	Date	Links
Malaysia	20 people	15 Apr 2016	https://www.taipeitimes.com/News/taiwan/archives/2016/04/19/2003644304 https://www.straitstimes.com/asia/east-asia/taiwan-says-china-seeking-deportation-of-taiwanese-from-malaysia-in-fraud-case
Malaysia	97 people	30 Apr 2016	https://www.china.org.cn/china/2016-04/30/content_38361649.htm https://en.people.cn/n3/2016/0501/c90000-9051860.html
Malaysia	74 people	29 Nov 2016	https://www.straitstimes.com/asia/east-asia/taiwan-protests-against-malaysias-deportation-of-fraud-suspects-to-china https://www.mac.gov.tw/en/News_Content.aspx?Create=1&n=2BA0753CBE348412&s=1E60D09B1EC1EB8E&sms=E828F60C4AFB AF90&state=F5D336F102ACBC68
Myanmar	1,207 people	5–6 Sep 2023	https://www.taipeitimes.com/News/taiwan/archives/2016/04/19/2003644304 https://www.straitstimes.com/asia/east-asia/taiwan-says-china-seeking-deportation-of-taiwanese-from-malaysia-in-fraud-case
Myanmar	2,349 people	Oct 2023	https://www.china.org.cn/china/2016-04/30/content_38361649.htm https://en.people.cn/n3/2016/0501/c90000-9051860.html
Myanmar	31,000 people	By 21 Nov 2023	https://www.straitstimes.com/asia/east-asia/taiwan-protests-against-malaysias-deportation-of-fraud-suspects-to-china https://www.mac.gov.tw/en/News_Content.aspx?Create=1&n=2BA0753CBE348412&s=1E60D09B1EC1EB8E&sms=E828F60C4AFB AF90&state=F5D336F102ACBC68
Myanmar	10 people	30 Jan 2024	https://www.theguardian.com/world/2024/jan/31/myanmar-hands-over-junta-backed-warlords-china-telecoms-scam-case-fraud-trafficking https://www.news.cn/20240130/74811813e22842208e258872411fdd3c/c.html
Myanmar	497 people	21 Feb 2024	https://www.globaltimes.cn/page/202403/1308010.shtml
Myanmar	352 people	31 Mar 2024	https://english.news.cn/20240401/07976c3e89a74b719b4302f7c183dff2/c.html
Myanmar	92 people	6 May 2024	https://english.scio.gov.cn/pressroom/2024-05/07/content_117170861.htm
Myanmar	150 people	Jun 2024	https://www.globaltimes.cn/page/202406/1314339.shtml
Myanmar	307 people	Aug 2024	https://www.globaltimes.cn/page/202408/1318442.shtml
Myanmar	111 people	13 Sep 2024	https://global.chinadaily.com.cn/a/202409/13/WS66e42b52a3103711928a7ef3.html
Myanmar	313 people	30 Sep 2024	https://english.scio.gov.cn/pressroom/2024-09/30/content_117461346.html

Country	No. of people	Date	Links
Myanmar	763 people	Nov 2024	https://en.people.cn/n3/2024/1122/c90000-20245757.html
Myanmar	2,876 people	20 Feb–14 Mar 2025	https://english.news.cn/20250315/892662f6ab0e4d6f92409b7ff0717b6b/c.html https://apnews.com/article/9fce90b60eb8cf5a42569f0e7ec865f6
Myanmar	more than 920 people	Apr 2025	https://www.globaltimes.cn/page/202504/1332705.shtml
Myanmar	1,178 people	9 Dec 2025 announcement	https://english.scio.gov.cn/pressroom/2025-12/09/content_118217833.html
Myanmar	952 people	16–19 Dec 2025	https://en.people.cn/n3/2025/1226/c90000-20407090.html
Myanmar	more than 1,500 people	Jan–9 Feb 2026	https://english.scio.gov.cn/pressroom/2026-02/10/content_118326395.html
Philippines	14 people	2 Feb 2011	https://www.mac.gov.tw/en/News_Content.aspx?n=14271038DDC4104F&s=BC2602F546AFBC9C&sms=E828F60C4AFBAF90
Philippines	73 people	27 Feb 2018	https://www.pna.gov.ph/articles/1027034 https://www.xinhuanet.com/english/2018-02/27/c_137003403.htm
Philippines	78 people	3 Apr 2018	https://www.xinhuanet.com/english/2018-04/04/c_137088209.htm
Philippines	36 people	7 Nov 2018	https://www.xinhuanet.com/english/2018-11/07/c_137589374.htm
Philippines	312 people	14 Nov 2019	https://www.pna.gov.ph/articles/1085996 https://www.gmanetwork.com/news/topstories/nation/715415/phl-deports-312-chinese-nationals-arrested-for-telco-fraud/story/
Philippines	75 people	22 Sep 2023	https://www.pna.gov.ph/articles/1210500
Philippines	417 people	By 20 Oct 2023	https://english.news.cn/20231020/30a4734b79374f56967f218ec60aeb00/c.html
Philippines	166 people	14 May 2024	https://www.pna.gov.ph/articles/1224726
Philippines	187 people	5 Dec 2024	https://www.pna.gov.ph/articles/1239430
Philippines	100 people	17 Jun 2025	https://www.pna.gov.ph/articles/1252332
Poland	1 person	6 Oct 2022	https://hudoc.echr.coe.int/app/conversion/docx/pdf?filename=CASE+OF+LIU+v.+POLAND.pdf&id=001-219786&library=ECHR https://www.refworld.org/jurisprudence/caselaw/echr/2022/124157
Slovenia	36 people	Jan 2018	https://www.helpnetsecurity.com/2018/01/23/defraud-chinese-computer-users/ https://www.taipeitimes.com/News/taiwan/archives/2018/05/05/2003692555

Country	No. of people	Date	Links
Spain	94 people	7 Jun 2019	https://www.euronews.com/2019/06/07/spain-deports-94-taiwanese-to-beijing-for-telecom-fraud https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Audiencia-Nacional/Oficina-de-Comunicacion/Notas-de-prensa/La-Audiencia-Nacional-concede-la-extradicion-a-China-a-121-ciudadanos-chinos-detenidos-en-la-Operacion-Wall-en-2016
Spain	1 person	29 Oct 2024	https://english.elpais.com/international/2025-05-25/spain-the-only-major-european-country-to-extradite-people-to-china-despite-the-generalized-violence-in-its-prisons.html?outputType=amp
Sri Lanka	125 people	29 Mar 2026	https://english.news.cn/20260409/1288580c1c124962bb5a90529c14e99a/c.html
Thailand	1 person	12 Nov 2025	https://www.theguardian.com/world/2025/nov/13/alleged-gambling-kingpin-she-zhijiang-extradited-thailand-china https://apnews.com/article/f19793e355e46b54f5df0a5398027eaf
Vanuatu	6 people	5 Jul 2019	https://www.rnz.co.nz/international/pacific-news/393732/chinese-nationals-deported-from-vanuatu https://www.abc.net.au/news/2019-08-07/vanuatu-passports-for-sale-scheme-to-chinese-nationals/11387292
Vietnam	19 people	By 26 Jun 2024	https://english.news.cn/20240626/b949f4250672451cb1fd8996cfafbcad/c.html

In contrast with the aggressive focus on extraditing scammers, China has placed little emphasis on novel technological solutions and has not made any effort to impose them on other nations. However, a new national authentication standard, GB/T 43779-2024, was published on 25 April 2024 with reported input from Samsung, the South Korean network manufacturer, as well as leading Chinese manufacturers, communications providers and academics [56]. The full title of the standard can be translated as “Technical Specification for Caller Identity Authentication Using Crypto Tokens”, but the official English abbreviation for this standard, CHAKEN, is a knowing play on the name of SHAKEN, the authentication standard promoted by US interests.

[56] State Administration for Market Regulation & Standardization Administration of China, GB/T 43779-2024 Cybersecurity technology—Technical specification for caller identity authentication using crypto tokens.
<https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=E23E1CA2CB5848D103B39C4C95700CCB>

CHAKEN is said to be backwards compatible with systems that have implemented SHAKEN but significantly extends the authentication process by creating cryptographically secure tokens that identify the phone user through software running on the user's phone instead of relying on the user's communication provider to vouch for the identity of its users. However, there are only modest signs of CHAKEN being implemented in practice. This may be because of concerns that CHAKEN could be interpreted as a surveillance mechanism by other governments or because the Chinese government is satisfied with the results obtained using other methods of verifying phone users and investigating crime.

China's diplomatic drive to coordinate international police action has recently accelerated with the publication by China's Ministry of Public Security of a mission statement for a proposed new "intergovernmental alliance against telecom and cyber fraud" [57]. Per their plan, the new alliance would consist of a plenary assembly that represents member states, an executive committee elected by the assembly to execute the assembly's resolutions, and a permanent secretariat that would be based in China. The goal would be to agree on a new international convention that covers the sharing of intelligence, the extradition of suspects, recovery of the proceeds of crime, and technical standards to transmit anti-fraud data and upgrade anti-fraud technologies.

China's diplomatic proposals have only received a muted response so far. It was announced that the plenary assembly would be held in China before the end of 2026, but it does not appear that many other major powers have agreed to participate. Nevertheless, China's proposals address many of the issues that need to be covered by international agreements on how to trace illegal communications and how to act upon the information collected. That this is occurring in the midst of a trade war with the USA that has targeted China's leading communications providers and network manufacturers indicates the extent to which China wishes to be a world leader in determining how countries will cooperate in fighting networked crime.

THE UNITED STATES OF AMERICA

It is worth examining how the USA is tackling scam communications in depth because most of the lobbying of European governments and regulators on how to perform traceback and authentication comes from American businesses and their allies. While Chinese lobbying focuses on Southeast Asia, including countries with a heavy concentration of scam compounds, American lobbying focuses on Western economies, which are more likely to perceive themselves to be the victims of scams than the hosts of scam compounds.

In contrast to China and India, whose telcos have the most subscribers, the USA is home to three of the world's top five revenue-generating telcos: Verizon, AT&T and Comcast. This actually represents a decline in the relative ranking of US telcos, with AT&T and Verizon continuously holding the number 1 and number 2 positions for global telco revenues from 2013 to 2021. The scale of US telecoms revenues relative to the size of the population reflects a culture where a considerable amount of business is conducted by phone, and which has relatively relaxed laws on unsolicited business phone calls compared to European countries. This also permeates into the political realm, where it is legally permissible for American politicians to make unsolicited phone calls to people's home phones without consent, resulting in sharp rises in unwanted robocall traffic during election years [58].

[57] https://english.www.gov.cn/news/202509/19/content_WS68cca861c6d00fa19f7a28e4.html

[58] <https://www.prnewswire.com/news-releases/us-consumers-received-nearly-4-9-billion-robocalls-in-october-according-to-youmail-robocall-index-302299609.html>

Unwanted robocalls generate more consumer complaints for the US telecoms regulator, the Federal Communications Commission, than any other category. The most reliable estimate of unwanted robocalls, the YouMail Robocall Index [59], has consistently reported between 3.5 billion and 5 billion robocalls per month for every month since STIR/SHAKEN became mandatory in July 2021, with no discernible trend up or down. STIR/SHAKEN was presented as the cornerstone of the US strategy for protecting consumers from unwanted phone calls until it became clear that the results were far inferior to the promises that had been made publicly.

US metrics fail to clearly differentiate between calls that are unwanted but legal, telesales calls that are illegal but not fraudulent, and scam calls. This results in a sensitive political issue where voter discontent prompts significant bipartisan agreement from Republican and Democrat politicians about how to tackle robocalls but little measurable progress. Meanwhile, complaints to the FTC show a steady upward trend in consumer losses to frauds instigated by a phone call. Recent FTC figures show that consumer losses to frauds instigated by a phone call are consistently exceeding USD 100mn per month. Per the political narrative supplied to the public, these losses are routinely blamed on bad actors working from abroad, with the implication being that the USA is relatively powerless to reduce the total without outside help.

The law enforcement philosophy of the USA can be sharply contrasted with that of China because of how much emphasis has been placed on mandating communications providers to implement new technology and how few arrests have occurred as a consequence of using this technology. Describing the evolution of the American philosophy of enforcing laws against networked crime is complicated by the interplay of different interest groups within a democratic society and free market economy. However, the simplest way to comprehend the current American philosophy towards traceback and authentication begins by acknowledging the influence of Henning Schulzrinne, an internet engineer who twice served as the Chief Technology Officer of the Federal Communications Commission (FCC), the regulator of US communications providers.

Schulzrinne is one of the original designers of Session Initiation Protocol (SIP), the signalling protocol for communications carried by IP networks that have been steadily replacing the TDM technology used by PSTN networks that are nearing the end of their life. Schulzrinne also instigated the consumer protection work that was meant to reduce the number of unwanted robocalls received by Americans and which led to the publication of the Secure Telephone Identity Revisited (STIR) technical standard in 2014. STIR then led to other standards in subsequent years, including Signature-based Handling of Asserted Information Using toKENs (SHAKEN), Rich Call Data (RCD) and VERifiable Sti PERsona (VESPER). These standards are often informally and collectively labelled as ‘STIR/SHAKEN’ as if they represented a single coherent formula for tackling illegal voice calls, despite each new standard being developed as a partial response to the limitations of its predecessors.

[59] <https://robocallindex.com/>



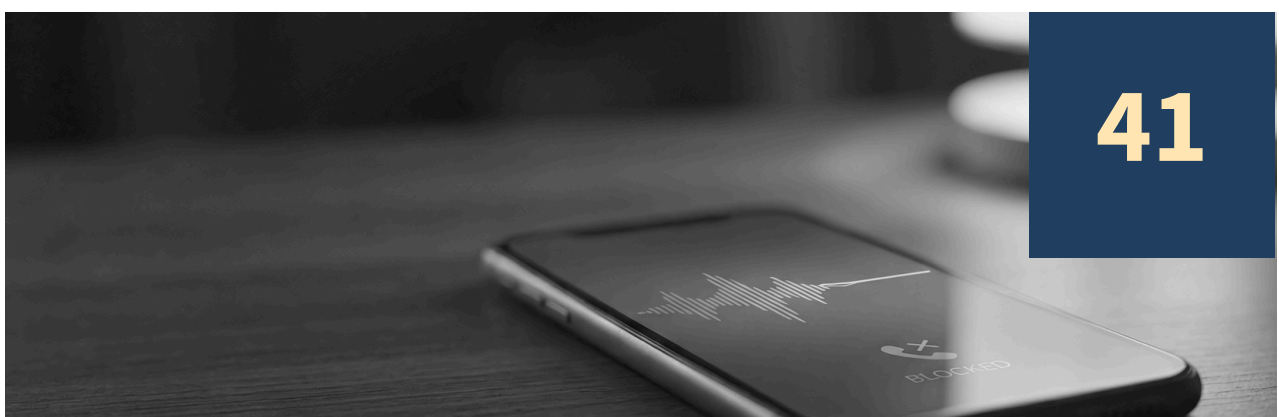
Focusing on the detail of these technical standards tends to blind naive readers to an even more important limitation of the STIR/SHAKEN umbrella approach: it only augments the verification and traceability of voice calls transmitted over IP networks using SIP signalling. This kind of electronic communication appeared to be the future of telephony, at least from the perspective that traditional telcos and their regulators would have adopted over a decade ago. This vision of the future did not anticipate the rising popularity of OCS channels of communication that represent competition for traditional telcos and which are often built upon proprietary protocols. OCS voice calls and messages are often preferred by scammers to reach their victims because of the end-to-end encryption (E2EE) that many of them offer. It is now common for scammers who instigate communication with a victim through a dialled voice call or an SMS to prioritise moving the conversation to an OCS channel as quickly as possible. This neuters the effectiveness of anti-scam controls that look for anomalous patterns of traffic for dialled voice and SMS. In addition to the increasing market share, there are also multiple examples of the hybridisation of OCS and traditional telecom services.

So instead of the Chinese approach, which works backwards from the general problem of crime and how to find who is responsible, the US approach started with a particular technological mindset and has then tried to match the development of that technology to how criminals behave in practice. This approach may face challenges because criminals are not constrained to communication channels aligned with the traditional telecom's technology roadmap.

Attempts to make a specific approach more general in its application have proven to be largely ineffective despite insider estimates that the US telecoms industry has collectively spent around half a billion dollars of capital expenditure on implementing STIR/SHAKEN. Even this figure may significantly underestimate the total cost of STIR/SHAKEN thus far, given that the FCC's own projections for the operating costs of STIR/SHAKEN ranged up to USD 780mn per annum [60]. This was justified at the time by the assertion that it was “implausible that the total implementation costs will come close to the expected benefits of our actions”, which were predicted to be worth “at least \$3 billion from eliminating illegal scam robocalls”. It is notable that there has been no desire to revisit the calculation of the benefits following the realisation that illegal scam robocalls have not been eliminated and that reported fraud losses have risen in the interim.

The absence of a single guiding principle for consumer protection is evident from the different claims made about STIR/SHAKEN by its own proponents. Some insist that SHAKEN can be adapted for use without STIR, thus making it applicable to networks that do not use SIP, while others insist that SHAKEN will only work in concert with STIR, and hence that all networks must be upgraded so every call is carried using a SIP VoIP channel from end-to-end. At different times, senior FCC staff have asserted that the purpose of STIR/SHAKEN is to show an incoming call is trustworthy (because attaching the data in a STIR/SHAKEN signature to a call results in a green tick being displayed on the receiving phone) and to facilitate more rapid traceback of bad calls. There is a contradiction in wanting to implement a technology to better trace calls that have already been proven trustworthy.

[60] <https://docs.fcc.gov/public/attachments/FCC-20-42A1.pdf>



The most severe problem faced by the current US strategy is that American consumer protection efforts focus so much investment on tackling inbound voice calls carried by traditional telcos, as part of a narrative that the blame for scams can be placed on foreign actors outside of US control. The narrow focus on SIP-based voice has seen less investment go into tackling the text messages sent by scammers or the use of OCS channels by scammers. Nor has sufficient effort gone into reducing outbound calls placed by the victims of scams, as can occur when a victim receives a message through another channel, such as an SMS message or a pop-up window on their browser, that directs them to urgently call the telephone number in the message. Recent regulatory changes have sought to enhance restrictions over the abuse of US phone numbers for outbound calls that are forwarded to scam compounds in foreign countries.

The relative failure of STIR/SHAKEN has prompted a series of other piecemeal initiatives to alleviate crime. These include:

- Increased use of artificial intelligence means of discriminating between suspicious and trustworthy inbound communications;
- Increased use of other anti-scam controls that have also been widely adopted across Europe, such as registers of telephone numbers that users cannot call because they are only intended for outbound calls from government or businesses;
- Requiring telecoms carriers that operate in the USA and which interconnect with those carriers to submit written explanations of how they mitigate robocalls to a national Robocall Mitigation Database; and
- Increased emphasis on foreign countries being to blame for unwanted communications received by Americans.

The push for increased international traceback from the USA is similar to the push for increased international cooperation with Chinese law enforcement agencies. It gives more prominence to the country's dependence on foreign cooperation than on the anti-scam options that remain wholly within the country's control. This is especially problematic in the USA because of the sparsity of prosecutions resulting from what is claimed to be a successful traceback mechanism.

The TRACED Act [61] gave the FCC new powers to punish businesses responsible for illegal robocalls and CLI spoofing when it passed into law at the end of 2019. The new law also mandated annual reports by the FCC to Congress that include statistics on how often the powers in the act had been exercised. As a consequence, we know that for the first five years the act has been in effect, the FCC has proposed and issued only eight fines for illegal robocall violations. The nominal value of these fines is impressive – over USD 700mn in total – but not a single penny was collected by the Department of Justice.

[61] <https://www.congress.gov/bill/116th-congress/senate-bill/151>

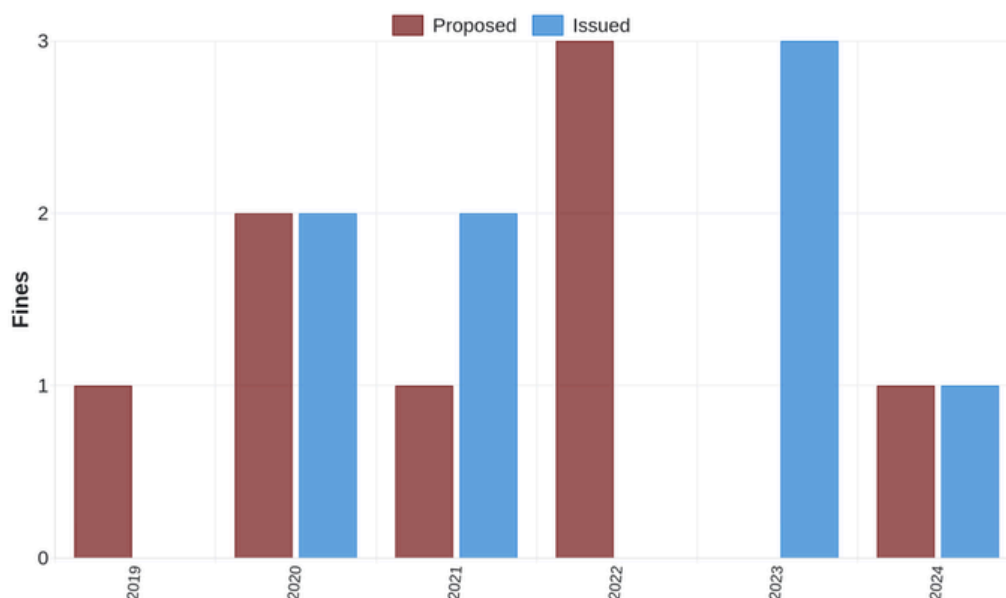


Figure 10: Annual Number of TRACED Act Fines Proposed and Issued [62][63][64][65][66]

Unfortunately, 2024 is the most recent year for which we have data from the official FCC report to Congress. For the last two years, the FCC has interpreted its legal obligation to provide Congress with an annual report about robocall mitigation as being satisfied by issuing a report in late December 2024 that covered 2023 and issuing a report in late December 2025 that covered 2024. The report including data from 2025 is hence only expected at the end of 2026. , This reporting approach may have reduced the visibility and timeliness of the published information, given that reports issued prior to 2024 included much more timely data.

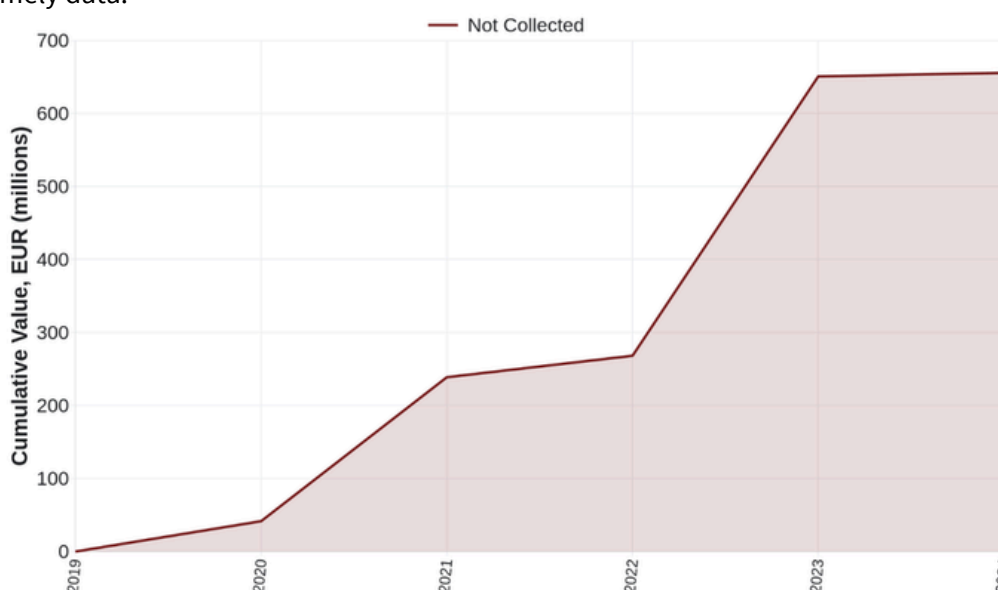


Figure 11: Cumulative Value of TRACED Act Fines Issued and Not Collected [67][68][69][70][71]

- [62] <https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2020-congress>
- [63] <https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2021-congress>
- [64] <https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2022-congress>
- [65] <https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2023-congress>
- [66] <https://www.fcc.gov/document/fcc-submits-traced-act-2024-annual-report-congress>
- [67] <https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2020-congress>
- [68] <https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2021-congress>
- [69] <https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2022-congress>
- [70] <https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2023-congress>
- [71] <https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2023-congress>

The number of prosecutions and enforcement outcomes appears limited relative to the scale of traceback activity described.

US prosecutors at the federal and state level have instigated very few prosecutions that fit the archetypal model that other countries are being encouraged to followed: identify a large volume of anomalous communications traffic, determine if the contents were a scam, execute a traceback, identify the A-party, prosecute the A-party. To substantiate this observation, we searched the quarter-million news announcements that detail prosecutions, verdicts and sentences on the US Department of Justice website. While there are plenty of stories about scams and scammers, only a few related to scam calls and messages being generated en masse. Even fewer were linked to extraditions of scammers from other countries. Only one explicitly referred to the work of the USTelecom Industry Traceback Group.

The scarcity of prosecutions within the USA is not due to a lack of data collected using traceback. Following a request by two US congressmen, the USTelecom Industry Traceback Group issued additional ‘transparency reports’ for each quarter from April 2023 to the end of 2024. These showed that the majority of calls they traced had originated with US businesses, as shown in the graph below. Only a small minority of the calls which were queried were traced to foreign CPs. There was also a clear trend over the period with the number of traces to domestic companies rising while the number of traces to international originators fell. This contrasts with a narrative that US prosecutors would like to take more action but cannot do so because most bad calls originate outside of their jurisdiction.

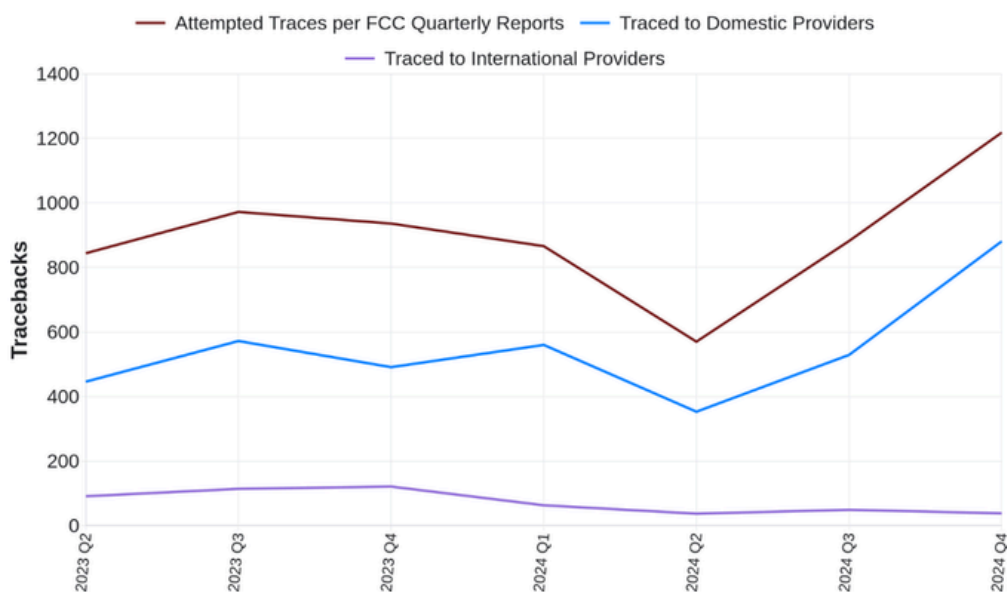


Figure 12: Tracebacks per FCC Quarterly Reports [72][73][74][75][76][77][78]

[72] <https://www.fcc.gov/document/fcc-releases-rollback-transparency-report>

[73] <https://www.fcc.gov/document/fcc-releases-q3-rollback-transparency-report>

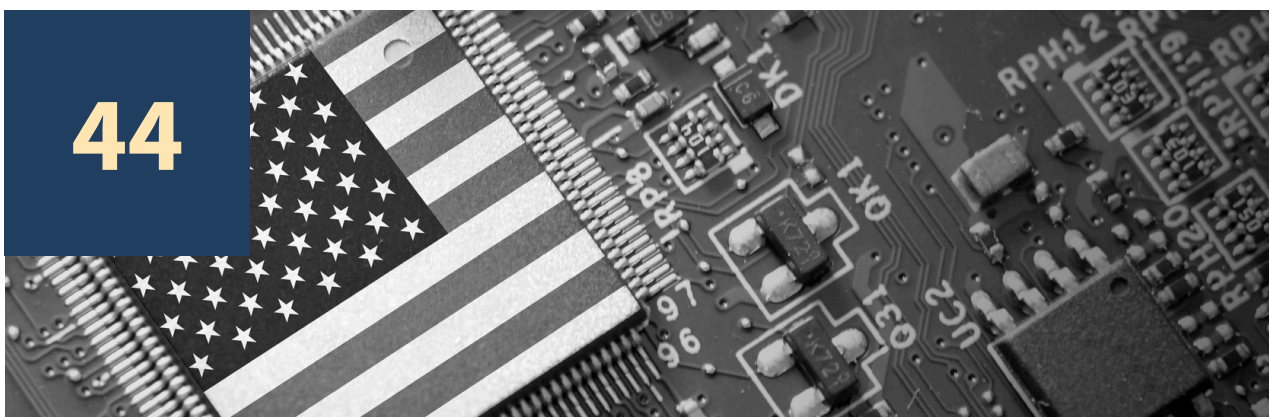
[74] <https://www.fcc.gov/document/fcc-releases-rollback-transparency-report-0>

[75] <https://www.fcc.gov/document/fcc-releases-rollback-transparency-report-1>

[76] <https://www.fcc.gov/document/fcc-releases-rollback-transparency-report-2>

[77] <https://www.fcc.gov/document/fcc-releases-rollback-transparency-report-3>

[78] <https://www.fcc.gov/document/fcc-releases-rollback-transparency-report-4>



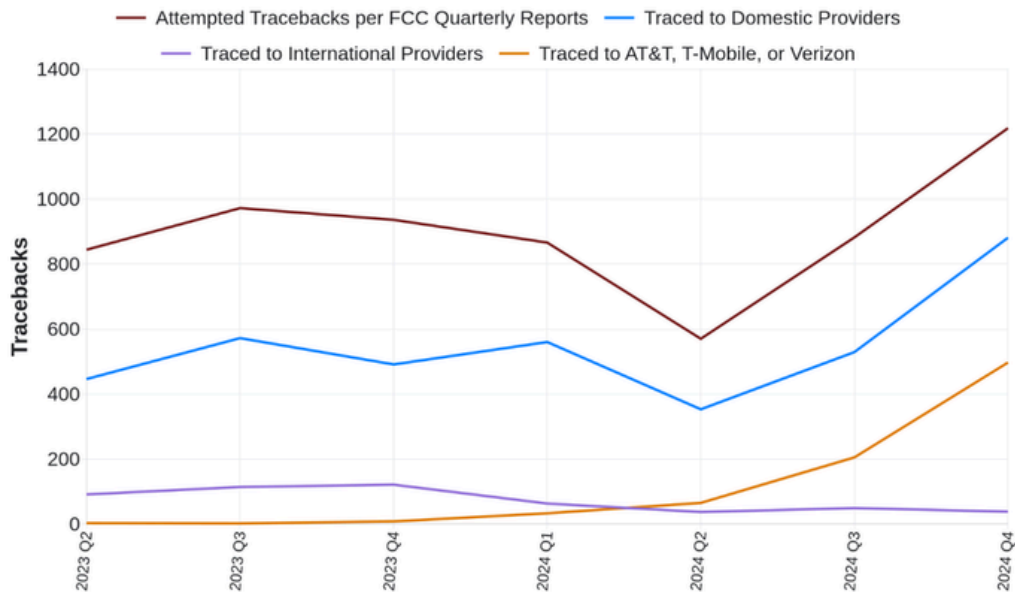


Figure 13: Tracebacks per FCC Quarterly Reports and Those Traced to AT&T, T-Mobile, or Verizon [79][80][81][82][83][84][85]

Subsequent annual reports by the FCC to Congress do not include a comprehensive table of which telcos have been most involved in tracing efforts, but digging into data presented for other reasons shows that over 9,000 traces have involved Verizon. Over 3,000 traces have involved T-Mobile USA when including figures for Sprint, which merged with T-Mobile USA in 2020. We could find no evidence of any other telcos being involved in significantly more than 1,000 traces, and only trivial numbers of traces that involved queries sent to European telcos. This begs the question of how much benefit would be generated by automating the process of supplying European trace data to the relevant US authorities.

Given the low return on the investment in systems meant to authenticate and trace calls, it may seem paradoxical that US interests continue to lobby foreign partners to follow the same approach. The USA has signed bilateral agreements to tackle robocalls and share intelligence with government agencies in Australia, Canada, Singapore and the United Kingdom as well as the EU’s Body of European Regulators for Electronic Communications (BEREC). This has been followed by a new law, the Foreign Robocall Elimination Act [86], which was passed by the US Senate in August 2026. It explicitly requires the formation of a task force comprised of American businesses and other organisations that are already advocates for the existing national strategy.

The objectives of the task force include:

- “examine methods for encouraging the adoption of caller identification authentication technology in foreign countries”

and

- “determine whether... it would be desirable to encourage other countries to adopt... the technical standards commonly known as “STIR/SHAKEN”

[79] <https://www.fcc.gov/document/fcc-releases-rollback-transparency-report>

[80] <https://www.fcc.gov/document/fcc-releases-q3-rollback-transparency-report>

[81] <https://www.fcc.gov/document/fcc-releases-rollback-transparency-report-0>

[82] <https://www.fcc.gov/document/fcc-releases-rollback-transparency-report-1>

[83] <https://www.fcc.gov/document/fcc-releases-rollback-transparency-report-2>

[84] <https://www.fcc.gov/document/fcc-releases-rollback-transparency-report-3>

[85] <https://www.fcc.gov/document/fcc-releases-rollback-transparency-report-4>

[86] <https://www.congress.gov/bills/119th-congress/senate-bill/2666/text>

The significant emphasis placed on the international promotion of STIR/SHAKEN and related authentication technologies raises questions regarding the factors supporting their wider adoption.

In addition to security and consumer-protection objectives, other factors may also contribute to stakeholder interest in STIR/SHAKEN.

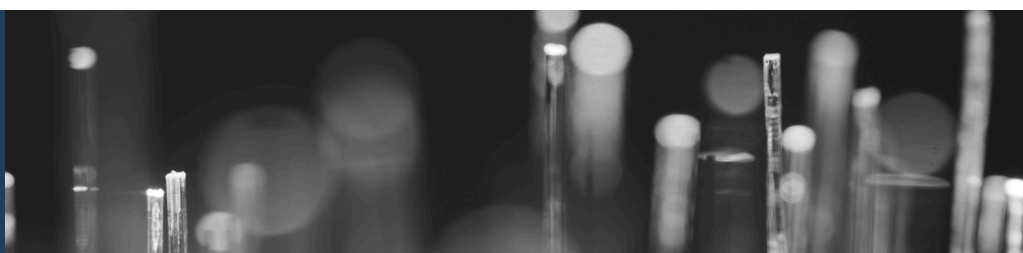
Beyond its authentication and traceback capabilities, STIR/SHAKEN may also support value-added services that create commercial opportunities for communications providers, particularly in markets where voice-based customer engagement remains important.

STIR and SHAKEN serve as a technological foundation for the delivery of additional services that can be sold at a premium to corporate customers that often use voice calls to speak to prospective and current customers. The data that authenticates a call can be augmented to also increase the chances of a phone user picking up; it is believed that showing a corporate logo and presenting the reason for a call on the display of a phone increases the likelihood that the call will be accepted by the intended recipient. This service is referred to as 'branded calling' and is treated within the telecoms industry as an adjunct to the same technologies as mandated for robocall mitigation in the USA. Juniper Research, a respected telecoms market research company, forecast in 2024 that the branded calling market would grow 3,318% between 2024 and 2029, resulting in annual revenues of USD 1.5bn [87]. The technological architecture adopted by the leading suppliers of branded calling assumes the adoption of STIR/SHAKEN or a similar framework in each country where branded calling will be implemented. This also assumes common international protocols where the branded calls cross national borders.

Branded calling can also be described as an anti-impersonation feature for those businesses willing to pay for it. It represents an especially valuable proposition in any market where telesales and telemarketing are common, or where it is conventional for services to be supplied over the phone. This explains why Brazilian telcos, which have telesales and telemarketing customs that are much like those found in the USA, voluntarily adopted a variant of STIR/SHAKEN. It also explains why traceback is usually discussed as an adjunct to authentication instead of vice versa. Profit can be generated by authenticating corporate users, but the technology needs to be supported end-to-end so the enhanced branding information is displayed on the phones of consumers.

It is debatable whether a similar combination authentication/traceback system would be as profitable in Europe, where there are more prohibitions on telesales and telemarketing, and where the population is less accustomed to receiving calls of this nature. However, the potential will still appeal to telco executives struggling to find ways to compensate for the ongoing decline in revenues from their core voice and SMS services. Law enforcement agencies should be wary of accepting a deal where they appear to have persuaded the private sector to deliver a new tool that will help the police to find criminals, but where the details of the design will make the system less effective at that task because a higher priority has been placed on features that can be marketed to corporate customers of communication services.

[87] <https://web.archive.org/web/20241020040628/https://www.juniperresearch.com/research/telecoms-connectivity/communication-services/robocall-mitigation-branded-calling-market-research-report/>



The US approach places strong emphasis on technology-led intervention, although questions remain regarding the relationship between technological deployment and measurable enforcement outcomes

This brings into sharp relief another difference in the way China and the USA address a key question: how much should limitations on police resources determine the amount invested in systems and processes to deliver traceback? A half-billion dollar system to trace calls seems profligate if there is only a negligible budget for the police tasked with acting upon the additional intelligence gathered, until we factor in the additional revenue streams generated by those businesses that have implemented the system. But if the system is designed primarily to generate revenue, instead of chasing criminals, there will be insufficient incentive to close the bypass routes that scammers will use to evade detection. A traceback and authentication system with 99% network coverage can be used to generate 99% of the potential revenue from branded calling, but will not track 99% of crime because criminals will adapt to preferentially use the 1% of routes that remain untraceable.

The possibility that bad actors may exploit gaps in the coverage of authentication is consistent with observations from the US market, where publicly available data indicate that adoption and end-to-end transmission of STIR/SHAKEN signatures remain incomplete.

According to monthly reports published by TransNexus, approximately one-third of calls currently reach their destination with an A-grade signature, indicating that the call was signed by the originating provider and that the signature has been successfully conveyed end-to-end. TransNexus also reports that this represents the highest level of A-grade signature coverage observed since the introduction of STIR/SHAKEN in the United States.

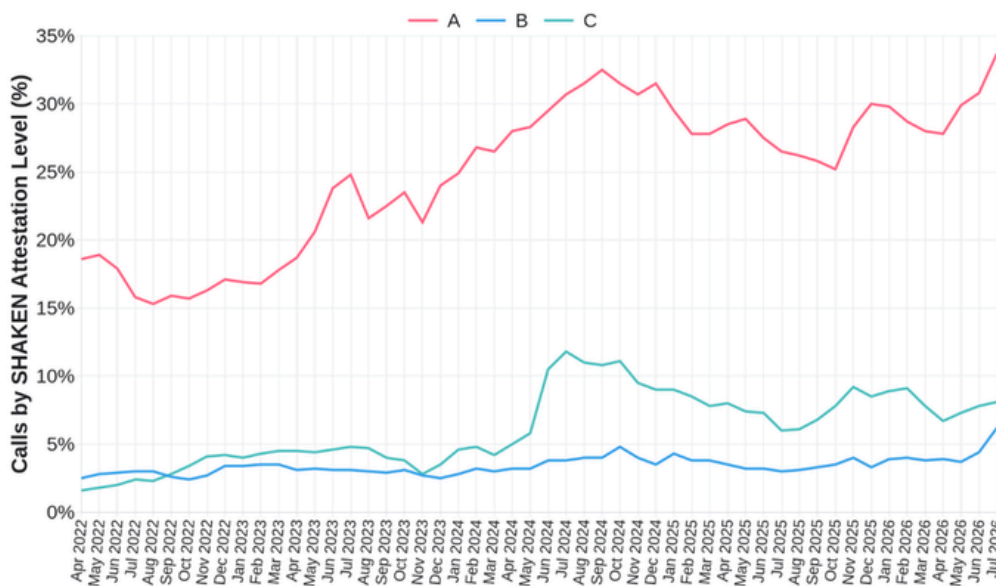
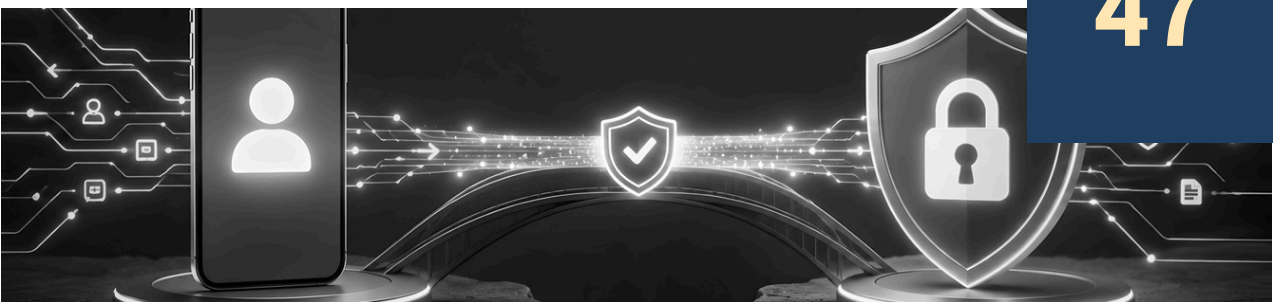


Figure 14: Monthly Percentage of Calls with an A, B or C-Class SHAKEN Signature at Destination per TransNexus [88]

Even including lower grades of signature, denoting that the call was not authenticated by the originating provider, July 2026 was the first month that TransNexus reported that more than 50% of calls reached termination with any class of SHAKEN signature.

[88] <https://transnexus.com/blog/>



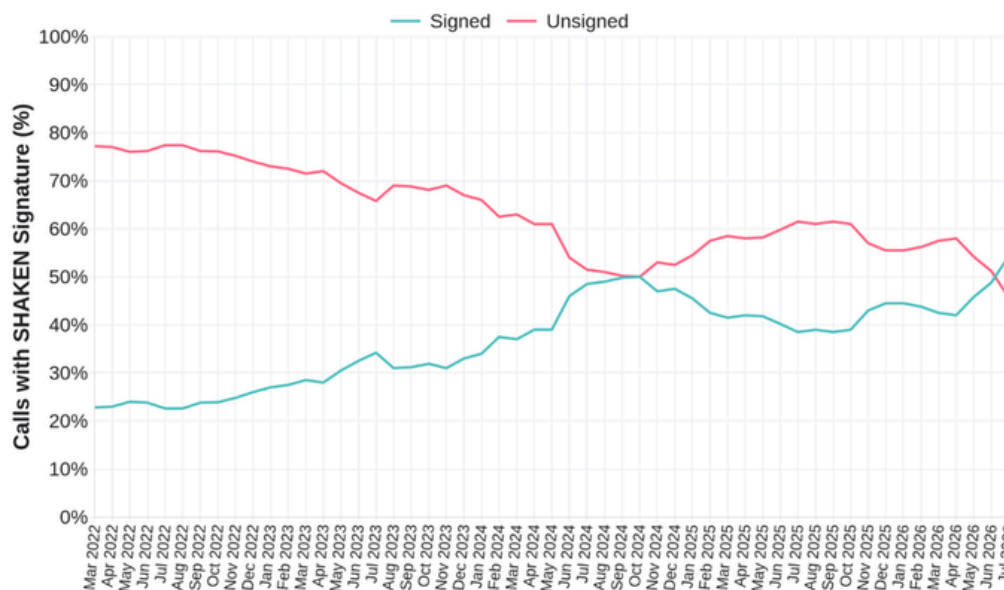


Figure 15: Monthly Percentage of Calls with Any SHAKEN Signature at Destination per TransNexus [89]

AN EMERGING THIRD WAY FOR EUROPE

The European Union has embarked upon a technological path that is distinct to China and the USA which will offer a radically different solution to the problem of how to authenticate communications and trace them to their origin. To understand the importance of this pathway, and why it clashes with the strategic objectives of other countries, we need to answer two questions that may seem so fundamental that they are unlikely to occur to anyone who is not a technology visionary: why do we use telephone numbers as the address of phone users and will we continue to use them in future?

Should People Be Identified by Their Telephone Number or by a Different Digital ID?

Even people with no curiosity about the past may be familiar with pictures of the original telephone operators: women who wore headsets and sat at desks with a wall of pinholes in front of them while holding wires with a plug at either end. These women would answer the calls of the phone company's customers, ask who that customer would like to speak to, then put the ends of their cables into the sockets to make a literal physical connection between analogue phone lines. Over time, the numbers on the grids they managed for each phone in a specific town were abstracted by adding more digits to represent different towns, and then different countries. Customers could start dialling the numbers of phones they wanted to reach in other towns and other countries without needing to speak to an operator, but the way this number was transmitted between systems was still analogue and mechanical. The number was sent as a series of electrical pulses, and intermediary machines would continue to make physical line connections by rotating and stepping the number of times iterated by the pulses in the numeric address. Germany and Switzerland only phased out their final electromechanical phone exchanges during 1997, 14 years after the production of the first commercially available mobile phone. During a period of transition from analogue to digital systems, an addressing system that worked with the old analogue systems continued to prevail. Now, as European countries near the retirement of all their PSTN networks and replace them with internet-based systems that are not only digital but also more flexible than the computerised systems they are also replacing, there is no logical limitation on how a communications addressing system needs to work in future. Put simply, it is not obvious how long we will continue to use phone numbers. Like the women who worked as telephone operators, they may rapidly become redundant because of changes in technology.

[89] <https://transnexus.com/blog/>

It was noted above that European countries, unlike the USA, already use alphanumeric sender address fields for Application-to-Person (A2P) SMS messages of the type normally sent by corporate users in bulk. China's CHAKEN protocols are predicated on the idea that a single user may have multiple personae and multiple numbers associated with a single phone – one persona may be for conducting business, another for their personal life – but the identity token produced by the software running on the phone represents the actual device, not any of the phone numbers used to receive calls at that device. The world is already familiar with the non-numeric addresses used for emails and websites. WhatsApp users see the usernames of other people they speak with, as well as their phone numbers, but WhatsApp will soon stop displaying the phone number. The list of examples goes on; the general trend is that phones, like other electronic devices, will increasingly be used for communications where the address is in a different format to the traditional phone number.

Telcos look at IP technology as a way to reduce their costs and increase the range of services they can provide, but they want to hold on to the old number-based addressing system because this gives them a competitive advantage. They have control of phone numbers. They know how to use phone numbers and how to obtain new ones. If everybody has to use phone numbers as the primary key for identifying an individual, then telcos will be able to generate revenue from their unique position in the market. They already leverage this advantage by generating revenue from the one-time passcodes sent by SMS to mobile phone numbers in order to authenticate a user's access to other online services, such as their bank account. It would suit telcos to continue to leverage their control of a global addressing system, even if they transmit the number-based authentication data in ways that are less visible to the end user than a passcode in an SMS. However, the EU has embarked upon a series of market reforms designed to open up the interoperability of online systems so there are many more ways that a user can authenticate themselves and gain access to online services. The EU's program is significantly more ambitious than anything currently envisaged by the USA.

These EU reforms are collectively referred to as eIDAS, standing for Electronic Identification, Authentication and Trust Services. The main driver of eIDAS is to liberate secure cross-border online transactions so less commission will need to be paid to corporations that enable the global use of credit cards and payment services. But the use of this authentication technology is not just limited to financial transactions. It can just as well be used to authenticate a phone user when he or she instigates a communication. As that capability becomes more widespread, it will beg the question of whether you primarily associate the phone user with their phone number or with a digital ID. There are advantages in associating the user with their digital ID, such as the fact that digital IDs can be used interoperably across other kinds of devices connected to the internet, instead of being so dependent on telephones.



As one of the goals of eIDAS is to improve authentication while reducing the costs multinational businesses, it would be odd for EU institutions to invest in systems that compete with eIDAS by being based on an alternative non-compatible identifier for each individual European citizen. This explains why the Global System for Mobile Communications Association (GSMA), the largest telecoms industry association, has a working group that is developing a technology called Open Verified Communication (OVC), an effective rival to SHAKEN which would also be interoperable with the addressing conventions made available through the adoption of eIDAS-compliant digital IDs. The potential of OVC has attracted the attention of other international institutions, such as the Global Legal Entity Identifier Foundation (GLEIF), which was created after the 2008 global financial crisis by central bankers, including the European Central Bank, to tackle challenges in correctly identifying banks that remotely work with each other. The Legal Entity Identifiers (LEIs) governed by GLEIF have now been adopted by a wider range of organisations and represent the kind of alternative source of identity that would be supported by OVC.

OVC currently has very little chance of being adopted in the USA because it is a competitor to SHAKEN. However, as its name suggests, OVC is an 'open' system that is meant to prevent control of authentication being dominated by a small clique of corporate entities. It is hence a better fit for the EU's technology roadmap.

OVC will be discussed further below, alongside the review of other methods to tackle spoofing. For now, the important point is that Europe is not following the same technology roadmap as the USA, nor has Europe devoted the same level of diplomatic resources to setting the agenda for international cooperation in tracing criminals as China. A simplistic analysis might say the EU is somewhere in the middle of these two superpowers. The EU has a more ambitious and more coherent long-term plan for the authentication of online users than the muddled situation in the USA, but with less obvious progress so far. There is more support within some European LEAs for traditional ways of gathering intelligence about criminals than that found in practice within the USA, but European countries are not giving police the same level of resources as the Chinese authorities. As such, the systems best suited to meeting the authentication and traceback requirements of European police will differ from those tailored to the needs and operating circumstances of police in either China or the USA.

NATIONAL SECURITY CONCERNS

Not all systems achieve the same quality of security or privacy for its users. When analysing the micro level of how a system may be subverted it can be easy to overlook macro-level risks pertaining to how a system is used in practice, how it is governed, the processes surrounding the technology and dependence on the suppliers of the system. This section briefly outlines some potential national security implications of implementing an EU-wide traceback and authentication system for communications, especially when this involves dependence on suppliers outside of EU control.

By its nature, a traceback system could be used to obtain sensitive data about phone users. Knowledge about conversations between business leaders could affect share prices; the reputations of politicians and other public figures may be damaged by revelations about who they have swapped messages with. The data obtained and retained by a traceback system should be managed according to the principles enshrined in the EU's General Data Protection Regulation (GDPR). This should mean that systems are designed to avoid the retention of data for unnecessarily long periods and that they maintain appropriate safeguards to limit who may access the data. It also means there is an obligation to understand the process being followed whenever data is being requested from the system, to ensure the request is both authorised and justified. Otherwise the privacy of the data collected by the system will be undermined by requests for information from people and organisations who do not intend to use it to uphold the law.

Salt Typhoon is an advanced persistent threat actor believed to be operated by China's state security which infiltrated telcos around the world and exfiltrated large volumes of data from those telcos [90]. Some of the telco systems subverted by Salt Typhoon were created to facilitate the supply of data to law enforcement agencies. It follows that an insecurely implemented traceback system would also be a potential target for hackers working on behalf of a hostile nation-state.

The effort involved in hacking a system can be eliminated if the system was intentionally supplied with secret back doors that permit unauthorised access. This is the rationale for several Western countries prohibiting the sale of certain categories of telecoms equipment made by Chinese companies. Some countries also require the removal and replacement of Chinese network equipment that has already been installed. Given the close relationship between the telecoms and surveillance industries, care should be applied to choosing the suppliers and reviewing the technology that will necessarily collect information about the authenticity, origin and destination of communications.

Tensions in international trade and the flaring up of trade wars poses a risk for systems that authenticate cross-border communications traffic. The telecoms industry already has a long history of ignoring the difference between blocking traffic because it is illegal and blocking traffic because it appears illegal. The distinction receives scrutiny when domestic traffic is blocked because of the realistic prospect of the wounded party invoking laws prohibiting monopolistic business practices. The distinction receives far less scrutiny for international traffic, especially when there is a significant imbalance in the power of the two countries involved. Where a centralised governance structure would control whose traffic is authenticated and whose traffic cannot be authenticated, their decision would have follow-on implications because of CPs that would selectively block unauthenticated traffic. So if the work of a centralised governance authority over international traffic is not conducted in a fair and impartial manner, the risk is that some business in some countries will be unfairly excluded from the communications ecosystem of other countries, or the burdens placed upon those businesses are not commensurate with the burdens placed on businesses and countries that are treated more favourably.

The risk of asymmetric sanctions is inherent to international trade, but the risk of outsourcing governance of the international trade in telecoms traffic to either private sector businesses or public institutions of foreign countries could easily be overlooked. In the worst case scenario, a major national telecoms provider could be put out of business because of the impact on its revenues from a decision to refuse the supply of a certificate to authenticate the telco's outbound traffic, leading to that traffic being automatically blocked by CPs that demand inbound traffic has been authenticated. In the context of a transnational governance body, the national telco cannot simply appeal to its own government that it was the victim of monopolistic business practices. It would have to appeal the transnational governance body, begging the question of how it is ensured that the transnational body exercises no favouritism in practice.

[90] <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a>



Some governance models overcome the risk described above. For example, OVC minimises the risks involved in cross-border governance because it is agnostic about which governance authorities will determine whether a communications business is allowed to authenticate a call or message. In effect, multiple governance regimes could freely be applied by OVC in parallel to the same communication at the same time. This can be visualised by imagining a telephone call where the handset displays a green tick denoting a valid signature per the governance authority in France, and a red cross denoting there is no valid signature per the governance authority in Germany, leaving the French recipient who is currently roaming in Germany to decide how to react. Multiple national authorities could work side-by-side without interference, and supranational governance bodies could also work in parallel or take over responsibility for a group of countries. This contrasts with the governance inherent to SHAKEN, which is designed to only have one central governance authority. With a centralised scheme, preventing the originating telco from signing calls can effectively mean their calls will be blocked by receiving telcos if those telcos insist on the valid signatures as proof the call is trustworthy.

The FCC evidently failed to appreciate the full consequences of outsourcing decisions to the STI-GA, the private sector consortium that acts as the governance authority for STIR/SHAKEN in the USA. They have ultimate power over granting or revoking SHAKEN certificates needed to attach STIR/SHAKEN signatures to phone calls. While the FCC made STIR/SHAKEN mandatory for calls on IP networks, they initially provided no route to appeal the decisions to refuse the supply of a SHAKEN certificate or to revoke an existing certificate. If the STI-GA effectively decided to eject a telco from STIR/SHAKEN then that telco would no longer be able to comply with the FCC's regulations, and this non-compliance that would make it legal for other telcos to refuse to accept traffic from the non-compliant telco. The risk of monopolistic abuse of the power of the governance authority evidently did not occur to the FCC until it was pointed out by telcos newly applying for SHAKEN certificates. The FCC then hurriedly rewrote its own regulations to turn themselves into the appeal body [91] for CPs denied a SHAKEN certificate.

Creating a route of appeal to the national regulator is an adequate compromise in the context of implementing STIR/SHAKEN within a single country with its own laws, but it highlights a key difficulty with internationalising SHAKEN: who would be represented on the governance authority deciding who can have SHAKEN certificates, and who would hear appeals if there was a dispute about the decisions made by that governance authority? If one country dominates the decisions of an international SHAKEN governance authority then this could be used as a backdoor mechanism to impose extraterritorial obligations on communication providers in foreign countries, or even to construct trade barriers by instigating blocking of communications from unsigned carriers in every country where a valid SHAKEN signature is a prerequisite of terminating a call. Such a mechanism would effectively be a multinational 'kill switch' for communications traffic from any telco that no longer received the approval of the transnational governance body.

[91] Federal Communications Commission. (2021). Call authentication trust anchor; Appeals of the STIR/SHAKEN Governance Authority token revocation decisions (Third Report and Order, FCC 21-93). <https://docs.fcc.gov/public/attachments/FCC-21-93A1.pdf>



The prospect of a transnational governance body for SHAKEN is not theoretical. The concept was described in 2020 within ATIS standard 1000091, Mechanism for International Signature-based Handling of Asserted Information using toKENs. The notional transnational governance body for STIR/SHAKEN was then launched on two separate occasions, though it never attained any meaningful role in managing international communications because its oversight role has only ever been acknowledged by American businesses.

In 2023, submissions to regulators in the UK [92] and Ireland [93] by US businesses including Google, Microsoft, RingCentral and Bandwidth referred to the existence of a ‘Cross-Border Call Authentication Governance Authority’ created by them in cooperation with ATIS. In these submissions, the role of the body was described as ‘non-jurisdictional’, but that elides the fact that withholding a trust mark necessarily has implications in any country where companies demand to see the trust mark before they will do business. The remit of the new international governance authority was clearly modelled on the remit granted to the STI-GA in the USA by the FCC.

A press release was then issued in August 2024 that stated ATIS, iconectiv, Bandwidth and Microsoft had collaborated to form a Cross Border Call Authentication Authority to tackle robocalls “on a global basis” [94]. The press release did not refer to the fact that this authority had previously been mentioned in submissions to European telecoms regulators. On each occasion, the businesses named as participants in the new governance consortium were exclusively American. This naturally leads to questions about how acceptable such a governance authority would be to foreign governments and regulators, not least because the USA and Canada had agreed a different framework for governing how STIR/SHAKEN applies to traffic between their countries.

[92] <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-2-6-weeks/260545-cli-authentication/responses/bandwidth-google-microsoft-and-ringcentral>

[93] <https://www.comreg.ie/media/2024/04/ComReg-2424s.pdf>

[94] <https://atis.org/press-releases/atis-iconectiv-trial-industry-robocall-initiative-with-bandwidth-microsoft-to-mitigate-unwanted-robocalls-globally/>



4 - APPROACH

54

The core of this report is a desk-based review of methods that can:

- Reduce spoofing;
- Authenticate communications; or
- Facilitate the tracing of communications.

Most attention has been directed to methods that have implications for both authentication and tracing, but their effectiveness has been put into context by also reviewing methods that tackle spoofing without seeking to authenticate traffic.

The research drew upon publicly available information from the following sources:

- Academic papers;
- Product marketing of businesses supplying relevant solutions;
- Formal technical standards where available; and
- Measures of the effectiveness of certain techniques per statistics published by police forces, regulators and businesses.

As far as possible, this was augmented by information that is not in the public domain.

- Information available to the author by participating in various telecoms industry forums such as the GSMA and One Consortium; and
- A new open online survey publicised using Commsrisk, a website with a global audience of professionals that have an interest in the topics covered by this report.

The online survey was created to reduce the risk that some relevant methods might be excluded from the report because they were unknown to the author and had not been extensively published or reviewed elsewhere. All the answers to the survey are documented in an annex to this report.

One of the ways methods were identified was by reviewing the work undertaken by several associations that have committed to finding or developing countermeasures to international scams. The work of those associations is covered in the following chapter.

One Consortium was the most productive starting point for compiling a comprehensive list of methods because they have maintained a working group tasked with compiling and updating a catalogue of 'tools' that can be used to tackle scams since the association was founded in 2024. Additional methods were then added to the review where identified by examining the work of other associations, online searches, personal interaction with relevant experts, or answers submitted to the online survey.

5 - INSTITUTIONS PURSUING INTERNATIONAL TRACEBACK

55

To understand the likelihood of anyone realising the goal of consensus agreement on how to perform international traceback, we examined the current status of work done by a series of influential and well-resourced bodies seeking to influence how traceback can be realised between communications providers in different countries. A global approach to tracing communications would require communications providers to coordinate their crime-fighting efforts to an atypical extent. So when considering which methods have a realistic chance of being applied globally, the methods fall into two groups:

- Methods that require significant intervention in the free market to attain widespread acceptance among communications providers within a single jurisdiction, and then significant diplomatic effort to ensure coordinated use by communications providers across multiple jurisdictions. STIR/SHAKEN is an example of a traceback method for calls that falls into this category.
- Methods that are so light, versatile and decentralised that businesses may voluntarily adopt them to solve specific problems and later agree to interconnect them. The GSMA's OVC is being positioned as a solution of this type in order to overcome some of the obstacles faced by STIR/SHAKEN.

Either way, there will be a need to reach consensus among a challengingly broad number of businesses, governments, regulators and police forces to deliver a global tracing system. At the time of writing, the organisations with a credible chance of leading efforts to build this consensus are:

- China's Ministry of Industry and Information Technology and Ministry of Public Security
- the GSMA
- the ITU
- One Consortium
- USTelecom

To anticipate which methods of international traceback may be cooperatively pursued by different countries in future, it is necessary to extrapolate from the work being done by bodies that have the resources or credibility to influence decision-makers in multiple countries. Each of the five leadership candidates are discussed below.

THE CHINESE MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY AND THE CHINESE MINISTRY OF PUBLIC SECURITY

It was mentioned above that China's Ministry of Public Security had published an ambitious manifesto for an international alliance to tackle telecoms scams. This referred to potential agreements covering intelligence sharing and anti-fraud systems. China's interest in locating and extraditing suspected scammers is obvious. However, the manifesto did not explicitly ask for the adoption of a global traceback system. China's influence over the development of a global tracing system must be inferred from other work conducted with the support of the Chinese authorities. This work primarily occurs within the ITU. Favouring the ITU for the ultimate standardisation of global traceback would be consistent with China's well-established preference for the governance of international networks to be overseen by a body working within the conventions of the United Nations.

Existing ITU work that could potentially feed into a global traceback framework tends to come from ITU study group 11 [95] and has been supported by China's Ministry of Industry and Information Technology as well as major Chinese telecom operators. The output of this study group includes ITU-T Q.3063, a standard on CLI authentication for voice calls, which builds upon the Q.3057 PKI standard by the same study group. Enabling oversight of this framework through the ITU or a new international entity would better suit China's diplomatic priorities than allowing governance to be influenced by nonprofit entities that govern other aspects of the internet and which are largely dominated by US and Western interests.

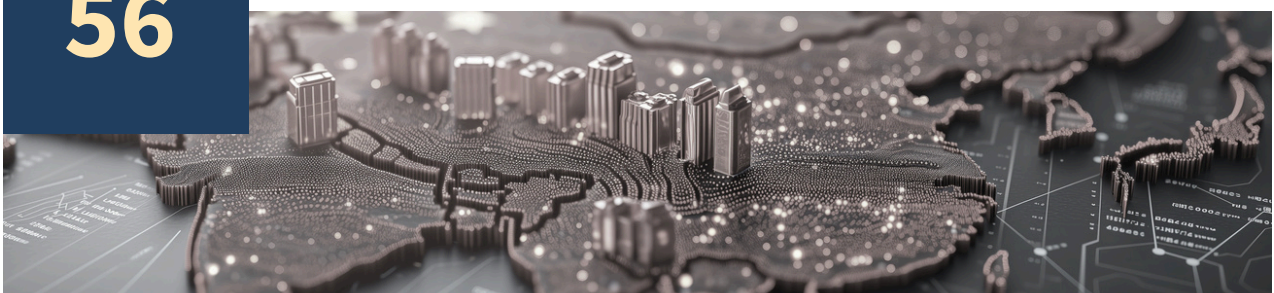
GMSA

The GSMA has made stop-start progress with technical questions relating to authentication and traceback. The seriousness of scams has forced the topic up the agenda of an organisation that has previously taken minimal interest in the topic, but a lack of an industry consensus prevents the GSMA from making substantive progress. Changes in personnel and uncertainty about where responsibility for scam prevention fits within their organisation chart have also impeded progress. The progress that has been made is usually conditional on there being a clear revenue-generating opportunity for one or more GSMA members and the absence of a conflict of interest with other GSMA members.

The first major substantive contribution from the GSMA was the launch of GSMA Call Check in September 2024 [96]. This was an out-of-band anti-fraud authentication and tracing service exclusively sold by the GSMA's Industry Services division. Call Check offered a rival conception based on the parallel out-of-band exchange of authentication and tracing data between communications providers, instead of data being transmitted in-band through SIP signalling. Despite the name, the capabilities of Call Check were not limited to voice calls and could be applied to other communication channels as well. Initial interest in Call Check was muted, and the GSMA relinquished their exclusive rights over the service in mid-to-late 2025, allowing the developer, a German business called Oculeus GmbH, the freedom to begin selling it directly to customers using the new brand name of Oculeus Two Factor Network (2FN).

[95] <https://www.itu.int/en/ITU-T/studygroups/2025-2028/11/Pages/default.aspx>

[96] https://www.gsma.com/solutions-and-impact/technologies/security/scams/gsma_resources/gsma-call-check/



A GSMA initiative entitled “United Against Scams” received more publicity in the run-up to the 2026 instance of the GSMA’s largest annual event, the Barcelona Mobile World Congress. In practice, the initiative appears to be a coming together of staff from several organisational divisions within the GSMA and representatives from some important GSMA members. Even the announcements of such an initiative would require coordination over time, but outputs have only been slight so far, probably because of the difficulty in reconciling the objectives of a wide variety of stakeholders. The GSMA’s output on scam prevention has been most overtly marketed to potential customers in the financial services sector, indicating a strong emphasis on revenue-generating opportunities created by communications providers supplying anti-fraud data or other forms of assurance to financial businesses.

Several senior employees of the GSMA involved in security, member coordination and the marketing of anti-fraud services to the financial services sector were invited to complete our survey in the hope they would share recommendations from the United Against Scams initiative. None did so. We eventually received a message after the deadline for the survey had passed from Erin Willis, the GSMA’s new Director of Scam Prevention. Per her public profile, Willis was appointed to this role in May 2026, having previously worked in marketing for the GSMA and other technology businesses. Willis indicated that the GSMA would make announcements about the output from “United Against Scams” during the run-up to the March 2027 Mobile World Congress.

In contrast to “United Against Scams”, which appears to be an initiative that members can only join by invitation, the member-facing side of the GSMA is the fulcrum for Open Verifiable Communications (OVC), a member-led proof of concept. Previously entitled Open Verifiable Calling but then extended to cover text messaging as well as voice calls, the goal of OVC is to show how multiple companies can work together to show that a communication has been authenticated in a way that ties the authentication to an independent vetting agency so that only the organisation with the right to use the originating address is able to use it and present the recipient with a visual or aural confirmation that the sender has been authenticated. For OVC, the GSMA acts as a passive meeting place for the various parties demonstrating the efficacy of OVC in practice. However, if OVC proves effective, then it is likely that the GSMA will then seek a larger role in its management.

Given the lack of output from United Against Scams, OVC is the closest thing that the GSMA has to a current working proposal for how to perform traceback and prevent spoofing. The technology has potential but would need to be supported by more GSMA members than just the current working group to have a realistic prospect of mass adoption.



ITU

The work done within the ITU to tackle CLI spoofing has been mentioned above in the context of Chinese influence over a potential global traceback framework. Despite (or perhaps because of) Chinese support, few businesses and agencies from other countries appear to be actively engaged with this work within the ITU. The relatively high cost of participating in ITU study groups also creates an obstacle to broad and active involvement from the private sector. There are no signs that the work conducted so far is influencing how consumers are protected from scams in practice. Some of the ITU's work in this arena was delivered too late to influence communication providers that had already made technical decisions that rendered ITU recommendations redundant.

The truly global role of the ITU might be considered to give it a better prospect of engaging interest from relevant parties in developing economies instead of its work being dominated by the richer countries which are most concerned with being on the receiving end of scams. However, it is not yet acting as a proactive meeting ground where representatives of Africa and South America would negotiate cost-effective solutions that could be implemented globally and which would also be acceptable to Asian, American and European interests.

ONE CONSORTIUM

One Consortium is a recent offshoot of the i3Forum, an older association of international wholesale carriers founded by European former wholesale carrier executives. The two associations have separate memberships but they are legally the same nonprofit corporation. Although i3Forum has had a productive anti-fraud working group for over a decade, that work had been focused on frauds that target wholesale carriers, not on scams that cause losses for the general public. Mandates imposed on international carriers by the USA since the beginning of the 2020's, including the adoption of STIR/SHAKEN, presented a significant risk to international wholesale carriers because of potentially inconsistent or even contradictory obligations that might be imposed by different countries where each country has some jurisdiction over parts of the same international communication. The launch of One Consortium in March 2024 was a way to address these risks while increasing revenues for the umbrella corporation by creating a new association that might also appeal to consumer-oriented telcos with no reason to join i3Forum.

In practice, the telco membership of the new One Consortium association remains significantly smaller than the membership of i3Forum, and the most active new CP members in One Consortium are US telcos with a relatively small international wholesale footprint but a strong incentive to impose US obligations on foreign businesses to guarantee consistency for themselves. As a consequence, 9 of the 14 voting members of the governing council work for businesses that are either headquartered in the USA or are European subsidiaries of US businesses. 5 of the 9 non-voting council observers work for industry associations that either exclusively or predominantly represent the interests of US telcos. There is no significant representation on the One Consortium council of carriers focused on Asia, Africa or South America despite the i3Forum having members that serve those regions.

Competition between international wholesale carriers means they generate large revenues from large volumes of telecoms traffic while only being able to maintain very thin margins. Operating budgets for these businesses are relatively small and they are sensitive to additional costs imposed by regulation. As a consequence, One Consortium has only modest resources compared to the other entities discussed in this chapter. However, the active participants have good reason to seek effective compromises that will reduce the number of scams suffered by consumers without massively reducing the amount of traffic that they carry, as might occur if there was a surge in automated blocking because of a trade war or an international dispute between countries that have conflicting anti-scam strategies.

The leaders of One Consortium lack knowledge of consumer protection expectations except when supplied by its US members. Nevertheless, it has outperformed larger rivals such as the GSMA by orchestrating meetings of an impressively broad range of national telecoms regulators. These regulator meetings are referred to as the Global Informal Regulatory Antifraud Forum (GIRAF). GIRAF is especially well attended by European regulators. These meetings are a major selling point to businesses which seek to gain access and influence over regulators outside of the USA.

GIRAF was only set up with an 18-month lifespan, but progress made during that time has been inconsequential, resulting in the ongoing extension of its life. Although GIRAF was initially believed to be a time-limited exercise, it has emerged as the preeminent intercontinental forum for regulatory staff concerned with the reduction of consumer scams and is likely to become a permanent fixture.

Tracing international phone calls and mitigating CLI spoofing are key agenda items for One Consortium. This is not surprising given the origins of One Consortium and the interests of the US members that have already implemented STIR/SHAKEN. There is also a working group that tackles analogous objectives for SMS and RCS messaging, but there is far less interest in this topic among members and that working group's recommendations receive less attention.

Some members of One Consortium are keen to explore the revenue-generating potential of digital identity services. The work on digital identity will likely result in a long-term vision for how to trace and authenticate communications traffic. There is a prominent overlap in the membership of One Consortium's digital identity working group and participants in the GSMA's OVC working group, meaning it is highly likely that OVC will eventually be selected as One Consortium's European-friendly way of harmonising with the objectives that drove the adoption of STIR/SHAKEN in the USA without accepting as closed and centralised an international governance structure as proposed by American advocates of STIR/SHAKEN. OVC also has the advantage of being applicable to the SMS and RCS messaging services that interest European telcos more than their counterparts in the USA.

Output from GIRAF remains limited, probably because of the difficulty of persuading national regulators to compromise in the arena of protecting consumers from scams. Few regulators have staff with significant expertise or experience of how to tackle scams. National regulators also work within a political context where consumer protection goals are set by national governments, not by foreign parties. It is noteworthy that the name of GIRAF explicitly refers to its informality; some national regulators would refuse to engage in conversations on these topics if it could be suggested that decisions might be binding on participants. Even so, GIRAF evidently takes great care to emphasise its minimal output is only advisory.

Only one GIRAF document has been published that can be meaningfully described as a recommendation. That document was published in May 2026 and it nominally concerns CLI spoofing although the title – “on possibly regulatory measures to combat illegitimate CLI spoofing” – reiterates that no decisions have been made [97]. The document is short, at just 1,190 words including sections describing who GIRAF is and disclaimers about the non-exhaustive and non-mandatory nature of the recommendations. The main substantive recommendation in this document is a rewording of ECC Recommendation (23)03, an effective anti-spoofing control previously endorsed by the European Conference of Postal and Telecommunications Administrations (CEPT) that has already been widely implemented across Europe. This control will be discussed in more detail in the following chapter.

[97] https://oneconsortium.org/wp-content/uploads/2026/06/GIRAF_Spoofing_recommendation_2026-01-v1-Final-12-May-2026.pdf



USTELECOM

The United States Telecom Association (USTelecom) is a nonprofit corporation that collects around USD 19mn per annum in revenue from American telcos and spends most of its operating budget on maintaining a full-time staff of around 33 people. The salary of its Chief Executive is over USD 2mn. The biographies of its staff reveal many connections with the US government and the FCC. One of the functions performed by USTelecom is to be the monopoly provider of call traceback services within the USA. This division of USTelecom is styled as the “Industry Traceback Group”, although it theoretically can be replaced through a recurring competitive tendering process that was written into the TRACED Act and is orchestrated by the FCC at regular intervals. In practice, there is no likelihood of USTelecom losing its role as the traceback provider because of the absence of credible alternatives and because the wording of the obligations written into the TRACED Act was closely patterned on the work that had already been performed by USTelecom prior to that law being passed.

These factors make USTelecom significantly different to most of the other organisations seeking to shape a global framework for traceback.

- USTelecom has a tight focus on traceback as opposed to other methods for tackling scams.
- USTelecom can share detailed experience of coordinating tracebacks in actual practice.
- USTelecom exercises more influence over its national government and national telecoms regulator than any other private-sector entity discussed in this report.
- But in turn, USTelecom acts as a proxy for the US government and its agencies when lobbying other countries.
- USTelecom benefits from far more focused resources on lobbying for a global framework for traceback than any other private-sector entity.

There is a lot of overlap between the businesses that support USTelecom and the businesses that support other US industry associations with an interest in shaping anti-scam policy, such as the Alliance for Telecommunications Industry Solutions (ATIS), the organisation responsible for writing the standards for SHAKEN. To map all the relationships between large US contributors to American industry associations and American politicians with the anti-scam policies advocated by those associations and politicians would be an extensive piece of work. It is sufficient to observe that USTelecom acts as a de facto spokesman for how the US telecoms industry and its regulator would like the rest of the world to tackle network-enabled scams in general, and for its pursuit of an international traceback framework for dialled voice calls in particular.

All of these factors make it highly likely that USTelecom will exercise more influence over the development of international traceback norms than any other entity, even though it makes no claim to represent the interests of telcos outside of the USA. USTelecom is also in an advantageous position because it is not burdened by the need to seek compromises between a variety of different stakeholders representing different countries and cultures. As such, it is the only organisation that presents a consistent and well-formulated plan for how it would like other countries to perform traceback. The core of that plan is to encourage other countries to make more data available to satisfy queries instigated by US LEAs and other American stakeholders. A secondary goal is to support the current US domestic strategy for scam reduction by encouraging the widespread adoption of SHAKEN or a SHAKEN-like technology. Per their reasoning, this would streamline hop-by-hop tracing of international voice calls so USTelecom can instigate many more traces of calls that terminated in the USA. However, it is not clear why they believe hop-by-hop tracing is more advantageous for international traceback than the direct method of traceback supported by different methods of authenticating communications.

6 - REVIEW OF METHODS TO TRACE COMMUNICATIONS AND MITIGATE SPOOFING

61

There are ways to trace communications, ways to mitigate spoofing, and some methods that facilitate both objectives at the same time. To avoid a lot of duplication, this chapter will review all plausible methods of tracing international communications and mitigating spoofing that have been developed or are in development. These methods will be presented in order of their viability as options to reduce the amount of crime endured by residents of the EU.

The sheer number of methods precludes a detailed technical examination of each one. Readers should keep in mind that the majority of methods discussed in this chapter are in flux. A technology being developed by a business may have demonstrated its effectiveness under controlled conditions but still needs refinement to ensure it works with all the varieties of communications and networks that will be encountered worldwide. Businesses will also be naturally reticent about sharing exact descriptions of how a technology works and the upgrades they are currently developing.

Even technologies that are thoroughly documented by technical standards bodies can be in flux at a practical level. For example, the technologies imprecisely labelled as STIR/SHAKEN stretch from the first statement of STIR requirements published by the Internet Engineering Task Force (IETF) in September 2014 – a statement that only concerns CLI spoofing for dialled voice calls – to the (seemingly ignored) extension for text messages that came out of the IETF in December 2023, to the current work in progress on VESPER, a possible way to show that a phone number is only being used by the party with the right to use it. So even if some parts of a technology have cemented their use within actual telcos, other elements will remain unproven in practice. This review will cover the essential elements of each method and will not try to drown the reader in extraneous detail.

EVALUATION CRITERIA

Each method has been evaluated using the following criteria.

Criteria	Approach
Proven effectiveness so far	Whether there are real-world results from using the method in practice. If so, how much impact the method has had.
	A high score in this category means the method has been proven effective in real life and at scale.
Range of communication channels covered by the method	Can the method be applied to many different communications channels or only one? For which communication channels does the method work? Can it be extended to other communication channels in future?
	A high score in this category means the method can be applied to a wider variety of communication channels.
Range of uses covered by the method	A method that can also be used to fulfil other anti-fraud or commercial purposes will be more popular with telcos than a method that can only be used to trace communications or prevent spoofing.
	A high score in this category means the method should be attractive because it can be used to do many things at once.
Market readiness	Can telcos pay somebody to implement the technology today? Is there a range of suppliers they can choose from? Or is further development required before the method will be ready for mass deployment?
	A high score in this category means the method should be attractive because it will be easy to find suppliers of the technology or to obtain experienced advisors on how to realise the method.
Anticipated cost of implementation	The cost of implementing a method will depend on the specific circumstances of the telcos, the networks and the countries where it is implemented, but it is still possible to make generalisations about which methods are cheaper and which are more expensive. Cheaper methods have a better chance of being adopted universally while expensive methods will struggle for acceptance outside of rich countries.
	A high score in this category means the method is cheaper, and hence more appealing to the organisations that will pay for it.
Style of traceback	Whether the traceback (if applicable) is direct to the origin or hop-by-hop via intermediaries. Direct traceback is quicker and serves the goal of identifying the criminal parties responsible for illegal communications without any extraneous effort. Hop-by-hop tracing is slower, more prone to failure to reach the origin because of the obstacles involved in completing each hop, but better suited to enforcement regimes where the primary goal is to punish carriers for not blocking illegal traffic instead of punishing criminals for creating illegal traffic.
	No score is attached to this category. Readers should decide for themselves whether hop-by-hop or direct tracing is a better match to their needs.
National security	As discussed in a previous chapter, some methods invite national security risks.
	No score is attached to this category. Readers should decide for themselves how to mitigate any national security risks inherent to the methods reviewed.

SOME OBSERVATIONS ON THE DIFFERENCE BETWEEN TRANSPORTING DATA AND THE DATA BEING TRANSPORTED

Marketing-driven narratives may have contributed to confusion regarding the distinction between different technologies and implementation models. . Technologies are artificially grouped together as if they have to be used together even though separate choices can be made concerning the format of data to be conveyed and the method by which that data is conveyed. A simple analogy is to ask if an ordinary person shares a photograph or a text document with a friend using email or using Microsoft Teams. There are four possible combinations because there are two formats for the data being conveyed (e.g. a jpeg file for the photograph or a Word file for the text document) and two communication tools that are separate but which are both capable of transporting the data (email or Microsoft Teams). Big business often wish to group technologies together for their own convenience and to simplify the choices available to the market but that does not mean the combinations they prefer are the combinations that best suit the eventual users of the technology.

The following examples may help readers understand the full range of options available.

STIR versus SHAKEN

It is common to hear decision-makers without specialist telecoms expertise refer to STIR/SHAKEN as if it is one thing because they do not understand the distinction between the two components explicitly mentioned by name. When used together, STIR is a protocol that safely conveys data using the SIP signals that manage a call in-band. The SHAKEN standard defines data that is conveyed using STIR. STIR can be used to convey data adhering to standards other than SHAKEN. Data defined by SHAKEN can be conveyed using different methods to STIR. That STIR and SHAKEN are sometimes used together does not mean they always need to be used together.

In-band versus out-of-band

These are general concepts in telecommunications. Management and control data for a communication that is sent in-band uses the same network path and rests upon on the same underlying protocols as the content of the communication. Sending this data out-of-band just means it is sent using a separate physical path or channel.

Every method that is not in-band is out-of-band. That means there are literally an unlimited number of ways of sending data out-of-band, though not all will be effective in practice. The author has worked at telcos in developing economies where the out-of-band transmission for data for billing purposes involved downloading data from a phone exchange to a computer tape, carrying the tape by bicycle to the telco's main offices, and then uploading the contents of the tape to a computer. However, these days an out-of-band transmission will usually involve a separate route for transmitting data over the internet.



Out-of-band SHAKEN

A good illustration of the distinctions mentioned above comes with the July 2026 publicity for a new ATIS standard for the out-of-band transmission of SHAKEN [1].

Despite the marketing puff in the announcement, this new standard is not the first or the only way to transmit SHAKEN out-of-band because the notion of out-of-band transmission is not limited in nature. But this is a method that gets the approval of ATIS and which is meant to be interoperable with the transmission of SHAKEN over STIR.

Rich Call Data (RCD)

RCD is often unhelpfully described as a part of the STIR/SHAKEN ‘family’ of protocols. But a more precise description would emphasise this is an additional protocol that defines information that is of use when identifying an inbound caller and which can be transmitted using STIR but does not have to be transmitted using STIR. To wrongly suggest RCD can only work in concert with STIR/SHAKEN is like suggesting SHAKEN can only work in concert with STIR.

OVC

Early marketing for OVC suffers many of the same defects as descriptions for STIR/SHAKEN, encouraging confusion in the minds of inexperienced audiences. OVC is an alternative to SHAKEN. Like SHAKEN, OVC does not define which protocols are used to transmit the data defined by OVC. Early proofs of concept for OVC have used STIR as a transmission layer, so if the naming conventions were consistent then this would be called STIR/OVC.

The promise of out-of-band OVC includes the prospect of applying OVC to SMS messages as well. This means the out-of-band protocols used in conjunction with OVC will likely differ for different communication channels being authenticated.

Transmission and governance

Readers without technical expertise often confuse the cryptographic security of transmitting data with the kinds of security they are actually interested in. Technologies to ensure data cannot be corrupted or manipulated during transmission are mature and readily implemented in practice. But just because data is not corrupted or manipulated during transmission does not mean it can be trusted. The well-known computing phrase of ‘garbage in, garbage out’ encapsulates the key problem. It does not matter how secure a transmission system is if the data entered into the system for transmission is wrong, dishonest, corrupt, garbage, etc.

[98] <https://atis.org/press-releases/new-atis-standard-to-extend-shaken-caller-authentication-across-tdm-networks/>



The FCC has been repeatedly caught out by this basic distinction. US authorities have often asserted that a call will be trustworthy if there is a STIR/SHAKEN signature attached. When speaking in favour of the TRACED Act and the provisions that mandated STIR/SHAKEN, Senator John Thune said in December 2019 that:

- *“This legislation will finally provide American consumers with the peace of mind they deserve when their phone rings... It equips carriers with the tools needed to verify caller ID and stop these calls before they reach your phone.”*

Ajit Pai, FCC Chairman in February 2020, reiterated the same claim when he said:

- *“Caller ID authentication is the key to restoring confidence in the phone network... Consumers will finally be able to trust the information displayed on their phone screens.”*

Neither of these statements was true, as vividly demonstrated on some of the rare occasions when the FCC tried to enforce its anti-spoofing rules. For example, thousands of registered voters in New Hampshire received calls in January 2024 that deepfaked the voice of President Joe Biden, telling them not to vote in the primary to decide the Democratic Party’s candidates in the general election later that year. The calls received an A-grade STIR/SHAKEN attestation despite spoofing the CLI of a well-known Democratic politician in New Hampshire. The case was settled out of court without the defending telco admitting to violation of FCC regulations. Their position was that it was mandatory to apply STIR/SHAKEN signatures to calls originating on an IP network, but there was no effective mandate stipulating KYC checks for the CLI and the identity of the originating party. The FCC has this year proposed a series of reforms intended to close this KYC loophole.

SOME OBSERVATIONS ABOUT SETTING ARTIFICIAL LIMITS ON TRACEBACK

It follows from the above that a desire to limit the transportation layer to a voice-only technology has biased thinking about the way to perform traceback. If a voice-only transportation layer is chosen then it is then argued that only the traceback of voice is required to tackle crime. This is fallacious reasoning. The correct sequence would involve determining which communication channels will need to be traced, and then to determine the one or several technologies that will be implemented to trace communications conveyed by those channels.

The single most common obstacle to thinking openly about which communication channels should be traced comes from the mistaken belief that commercial or jurisdictional limits on the interests of intermediate decision-makers represent technological limits on what is possible. For example, national regulatory authorities for telecommunications are often treated as having special domain expertise that is pertinent to the tracing of electronic communications and hence may have an outsized influence over decisions relating to the way technology is used to trace criminal communications. However, those same authorities typically have legal limits on their scope of responsibilities so they are only responsible for a narrowly-defined group of traditional telecoms services that have been dominant and which are in decline (voice, SMS messaging) and not for newer communications services enabled by the internet but which remain outside of their jurisdiction (RCS messaging, proprietary voice protocols such as WhatsApp, proprietary messaging protocols such as iMessage).



Similar constraints on thinking occur when asking businesses that are considered expert in the domain to share their advice. They may only have a commercial interest in certain forms of communication (such as SMS messaging) or certain technologies for managing voice channels (such as SIP signalling for voice). Employees of telcos who may be considered knowledgeable in this domain because they are SIP engineers can be placed in a position where they influence opinions about matters beyond their remit within the workplace (such as the extent to which WhatsApp is used to facilitate crime).

To avoid bias, the onus must be on law enforcement agencies to describe the priorities for fighting crime without any reference to design choices that would influence which technologies will be used, and hence which crimes cannot be tackled because they lay outside of the bounds of what that technology can do. For example, is it a priority to tackle crime propagated using SMS messaging, or crime propagated using any text messaging protocol that is presented in the same way to the end user? The latter includes RCS messaging and iMessage, and there is already plenty of experience showing that criminals have been using these latter channels to work around anti-crime controls that have only been implemented for SMS.

This question about priorities relates not just to historic and current data about the methods used by criminals but also forecasts for how crime will be conducted in the near future. Given the timescales for the comprehensive implementation of new systems and processes that would satisfy goals such as international traceback across all EU countries, there is a significant risk that the methods used by criminals will have significantly evolved before the project would be complete. For example, if it is announced that the EU was to implement a comprehensive framework for tracing all criminal SMS communications back to its source, then it would be highly likely that crime conveyed by text messaging would mostly switch to RCS and iMessage before the ability to trace SMS was in place across all relevant businesses and all EU countries.

This report cannot tell law enforcement agencies how much they should anticipate the use of newer communications channels when setting expectations for systems that will trace communications across international borders. It can, however, observe that there is copious evidence of criminals already migrating to newer channels (WhatsApp, iMessage, RCS) in response to enhanced anti-crime controls over older channels, and that much of this evidence comes from data published by national authorities within Europe. The evaluations given below will seek to give some weight to the importance of tracing and authenticating communications across channels that may be considered newer but whose popularity with the public is already considerable. Readers will need to decide for themselves if too much or too little weight is given to the importance of protecting consumers from the abuse of those channels too.



DETAILED REVIEW OF METHODS

The methods reviewed in this chapter are not ordered alphabetically or by the chronological date of when they were first conceived or implemented in practice. Such an ordering system would be relatively meaningless and lead to the inconsistencies inherent to reviewing completely new and unproven methods as if they can be treated just like methods that have been extensively implemented in practice, and for which there is considerable data to help us judge how effective they are actually are. The methods in this chapter are reviewed in order of the impact they have already had, starting with the most impactful first.

Table 6: Summary of Evaluation Scores for Each Method

Method	Proven Effectiveness	Range of Communication Channels	Range of Uses	Market Readiness	Anticipated Cost	Overall Score
Blocking inbound international calls that spoof a domestic phone number; ECC Recommendation (23)03	10	2	1	9	10	32
SMS Sender ID registries and other registries based on the originating address of an A2P text message	9	2	2	9	8	30
Blocking of calls that spoof a phone number on a national do-not-originate list	10	1	1	9	9	30
Blocking of calls that spoof an invalid, unallocated or unassigned phone number	7	2	4	7	9	29
STIR, SHAKEN, RCD and VESPER	5	2	8	9	0	24
Out of band SHAKEN	4	6	7	7	5	29
Origem Verificada	9	1	1	10	8	29
Oculus 2FN (previously known as GSMA Call Check)	4	10	10	2	9	35
CHAKEN	1	3	7	1	0	12
AB Handshake	3	5	5	3	10	26
OVC	4	5	5	3	10	27
CIV	3	2	2	2	10	19
CodeB Sovereign SBC	Not enough information to give a fair evaluation					
ITU-T Q.3063	Not relevant to deciding the future of call authentication in the EU					
Heksagon Call Verification Services	Outside the scope of this review					

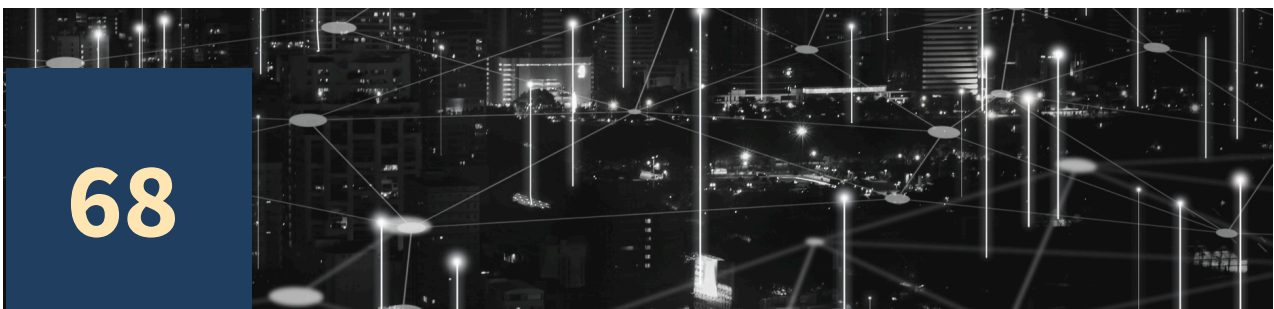


BLOCKING INBOUND INTERNATIONAL CALLS THAT SPOOF A DOMESTIC NUMBER; ECC RECOMMENDATION (23)03

This method has no brand name, is not defined by a technical standard published anywhere in the world, has never been promoted by any association of telcos, and has never been marketed or sold by any vendor. But it comes first in this review because the blocking of inbound international calls that spoof a domestic phone number has made a greater contribution to the reduction of spoofed scam calls than any other method. It is cheap and simple and already being used in many European countries. Some national implementations still need enhancement to attain their full potential but the sooner this method is comprehensively realised across the European Union, the safer Europeans will be. Prevention of crime is better than tracing crime and this is the simplest preventative measure with greatest effect for dialled voice calls. Other methods are far less effective and should only be considered after this control has been realised in full. The method is so impactful and so cost-effective that it dramatically alters the cost-benefit calculations for other anti-scam methods by significantly reducing the potential benefits they can deliver.

A basic outline of the control is sufficient to explain how it works and why it is effective for tackling scams. Most countries find that the majority of scam voice calls originated abroad. When a scam call from a foreign country spoofs a CLI to impersonate a business or person within the country then it presents a domestic phone number instead of a foreign phone number. The content of the number makes it generally easy to detect the mismatch between the use of an international line for the call and the apparent domestic status of the A-party. Blocking calls that exhibit this mismatch leads to a dramatic reduction in spoofed calls because it eliminates all spoofed calls that do not originate within the country.

Despite its simplicity and effectiveness, this method is opposed by some telcos because its effectiveness stems from how much it reduces the amount of international voice traffic that is connected, thus reducing the revenues of voice providers that serve wholesale and enterprise customers. It also increases the costs of businesses that primarily serve customers who originate communications from offshored call centres because of the need for additional verification that those customers are legitimate and that they only generate legitimate traffic. International enterprises are an important source of revenue for some telcos due to the decline in other revenue streams. The need to protect the general public from harmful controls has sometimes been given a lower priority than the desire to serve businesses that wish to call prospective customers from offshored call centres. The burden of proof should be on those parts of the telecoms industry that serve foreign and offshored business operations to demonstrate they can safely distinguish between the legitimate and illegitimate spoofing of calls, beginning with enforceable KYC standards that penalise communications providers who choose to serve bad actors. This is a challenge the telecoms industry has failed to adequately address in practice.



The effectiveness of blocking inbound international calls that spoof a domestic number is best illustrated by publicly-available data from the United Kingdom, an early adopter of this control. The data from the UK is especially revealing because it shows a strong correlation between the timing of the adoption of this control and public reports about unwanted calls during a period when no other major changes in anti-scam controls were being implemented by telcos. The following graph shows complaints made by the public to the Information Commissioner's Office (ICO) about unwanted live and automated calls. The rapid rise in complaints about automated calls coincided with increased scam robocall activity during early stages of the COVID-19 lockdown. The sharp 81.2% fall in monthly complaints between March and August 2021 coincided with major UK telcos voluntarily implementing blocks on inbound international calls spoofing domestic numbers. Subsequent regulation refined these voluntary controls and made them mandatory but the complaints data indicates that all of the impact was realised during the initial voluntary phase of adoption and that little has changed since.

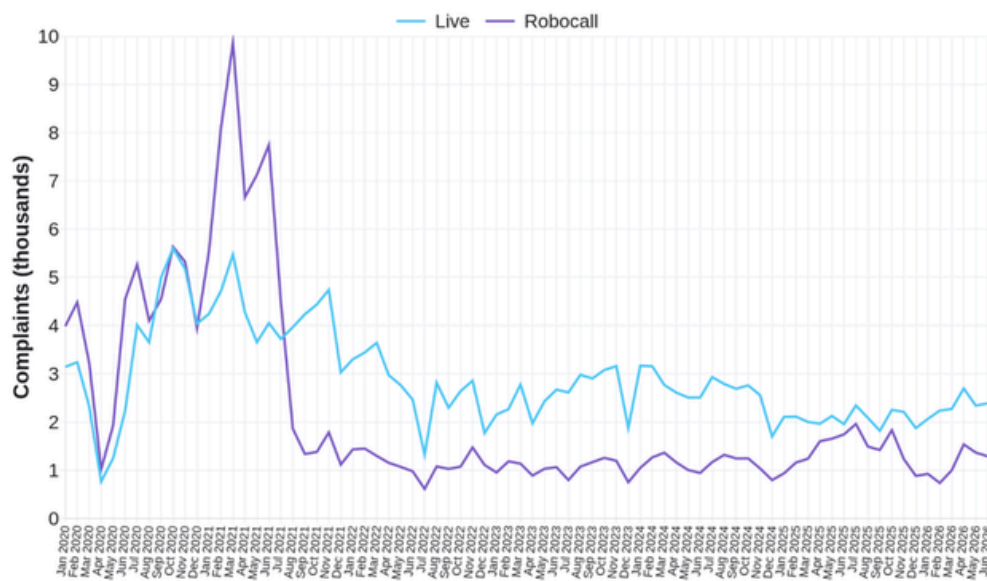


Figure 16: Monthly Complaints about Live and Automated Calls per ICO [99]

Other countries have reported similar levels of success after adopting this control. For example, India's Minister of Communications, Jyotiraditya Scindia, praised the control shortly after it was introduced, saying:

- *“Through the CIOR [Centralized International Our Roamer] software, we were able to block around 1.35 crore [13.5 million] such calls per day. Today, all those spoofing gateways have been blocked, and the number of spoof calls coming into India has reduced by 97%, down to just 3.3 lakh [330,000] calls a day.”*

Data published by the National Communications Commission of Taiwan in 2023 stated there had been a 70% reduction in the number of incoming international calls after the regulator instructed telcos to block international calls presenting a domestic phone number. The number of inbound international calls went from 51 million in May 2023 to just 15 million in October 2023.

[99] <https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/nuisance-calls-and-messages/>



The Finnish Ministry of Justice gave its 2025 crime prevention award for a system to block spoofed inbound international calls developed by Traficom, the national telecoms regulator, in cooperation with Elisa, a Finnish telco. Per the information given in the announcement of the award:

- *“Before the introduction of this solution, falsifying a caller ID to make it appear Finnish was one of criminals’ main tactics for making scam calls seem credible. As many as 90% of calls from abroad to Finnish numbers used falsified caller ID information. Thanks to the cooperation between Elisa and Traficom, the number of scam calls first fell to about ten per cent and then further down to three per cent.”*

Blocking inbound international calls that spoof a domestic phone number is cheap, though the exact cost dynamics depend on the way a country has structured its number ranges. If a country uses clearly separate number ranges for landline and mobile calls, then the identification of international calls that spoof a landline number is trivial. Most countries begin by immediately implementing blocks of calls that spoof domestic landline numbers while working on the systems required to safely block calls that spoof domestic mobile numbers.

Controls over calls that present a mobile number as the CLI need to be more sophisticated because legitimate phone users will originate calls presenting a domestic CLI when they call back to their home country while they are roaming abroad. To prevent the blocking of legitimate calls, telcos in the home country also need to perform a check to ensure the phone user is not roaming at the time the call from their number is received. This is typically referred to as a ‘roaming status’ check or an ‘is-roaming’ check. The check involves processes and systems so mobile network operators can pool or query roaming data from other mobile network operators within the same country, so none inadvertently blocks calls from a customer of another domestic network. Different countries have developed or are developing a variety of methods for sharing the data involved in a roaming status check. The GSMA has also proposed methods to check the status of roamers.

A slight variation of this control over inbound international calls involves ‘soft blocking’. Soft blocks occur where the communication is still connected but the recipient receives a warning or other sign that leads them to reject the communication, or where the communication is directed to the equivalent of a ‘junk’ folder instead of being treated like other communications. Care is needed with soft blocks. They shift legal liability so that the parties implementing the soft block may not be legally liable for the customer’s decision to reject the communication. However, they tend to be almost as effective at interrupting communications as literal blocks, so have similar consequences if a legitimate communication has been incorrectly flagged.



Soft-blocking in the context of this particular control involves suppressing the CLI instead of preventing the call being connected. Recipients are not shown any phone number for the incoming call and they may be shown words that effectively state that the CLI was withheld. The available data, including anecdotal reports, suggests that soft blocking is almost as effective as actual blocking, because customers almost always reject calls where the CLI has been removed. In particular, the Austrian telecoms regulator, Rundfunk und Telekom Regulierungs-GmbH (RTR), announced that scam calls involving Austrian phone numbers “had decreased to a fraction of their previous level” as a consequence of removing CLIs from inbound international calls that would otherwise spoof a domestic CLI [100]. Per RTR’s figures, the average number of monthly complaints about unwanted calls from an Austrian phone number fell by 84.75% when comparing the eight months of 2024 preceding the control becoming mandatory on 1st September 2024 with the remaining four months of the year. This contributed to an overall 76.4% fall from 2024 to 2025 in the annual number of reports of Austrian phone numbers being misused, as illustrated in the graph below.

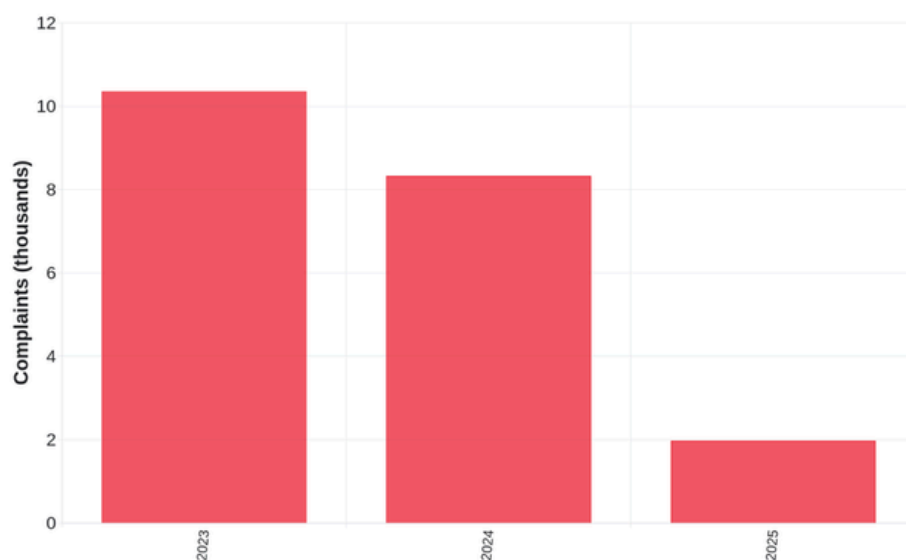


Figure 17: Annual Complaints About Misuse of Austrian Phone Numbers [101] [102]

Although there is no technical standard that defines this control, because the concept is so simple as to not require a technical specification, the principles for both the hard block and the soft block versions of this control are most fully described in Electronic Communications Committee (ECC) Recommendation (23)03 of the European Conference of Postal and Telecommunications Administrations (Conférence européenne des administrations des postes et des télécommunications, CEPT) [103]. CEPT is a coordinating body for European telecoms and postal regulators and currently brings together representatives of 46 European countries. ECC Recommendation (23)03 was published in November 2023 and drew upon the experience of how well the control was working in countries that had already adopted it.

[100] https://www.rtr.at/TKP/aktuelles/publikationen/newsletter/newsletter_2025/RTR.Telekom.Post-Newsletter_01_2025/teilerfolg-im-kampf-gegen-spoofing.de.html

[101] <https://www.rtr.at/TKP/aktuelles/publikationen/Uebersichtsseite.de.html?l=de&q=&t=category%3Dtaetigkeitsberichtslichtungsstelle>

[102] https://www.rtr.at/aktuelle_beobachtungen

[103] <https://docdb.cept.org/download/4402>



The recommendation is not binding on members but has been widely followed across Europe and by countries on other continents too. Based on our research, the following European countries have either mandated hard blocks of spoofed inbound international calls per ECC Recommendation (23)03 or have at least one major telco that has voluntarily adopted blocking based on this recommendation:

- Belgium [104]
- the Czech Republic [105]
- Estonia [106]
- Finland [107]
- Greece [108]
- Hungary [109]
- Ireland [110]
- Italy [111]
- Latvia [112]
- Lithuania [113]
- Luxembourg [114]
- Malta [115]
- Norway [116]
- Poland [117]
- Romania [118]
- Spain [119]
- Sweden [120]
- the United Kingdom [121]

[104] Belgian Institute for Postal Services and Telecommunications (BIPT), “A new step in combatting telephone fraud,” 6 June 2024, <https://www.bipt.be/consumers/publication/a-new-step-in-combatting-telephone-fraud>

[105] Czech Telecommunication Office, “Press Release: First anti-spoofing measures in force from 1 June,” 26 April 2024, <https://ctu.gov.cz/en/press-release-first-anti-spoofing-measures-force-1-june>.

[106] <https://news.err.ee/1610067550/government-seeks-mandatory-blocking-of-estonia-number-spoofing-scam-calls>

[107] Finnish Transport and Communications Agency (Traficom), “Obligations of the Regulation come into effect – up to 2,000,000 scam calls are prevented per day,” 22 November 2023, <https://www.traficom.fi/en/news/obligations-regulation-come-effect-200000-scam-calls-are-prevented-day>.

[108] https://www.eett.gr/deltia_tipou/lipsi-metrou-antimetopisis-tilefonikon-kliseon-apatis-me-ti-methodo-cli-spoofing/

[109] https://english.nmhh.hu/article/258169/Starting_the_summer_mobile_phone_numbers_will_also_be_harder_to_spoof

[110] Commission for Communications Regulation (ComReg), Tackling Nuisance Communications CLI Call Blocking Update, ComReg 23/47 (2023), p. 4, <https://www.comreg.ie/media/2023/05/ComReg-2347.pdf>

[111] Mobile Ecosystem Forum, “Italy’s New Agcom Regulation: A Turning Point in the Fight Against Telemarketing and Spoofing,” 29 July 2025, <https://mobileecosystemforum.com/2025/07/29/italys-new-agcom-regulation-a-turning-point-in-the-fight-against-telemarketing-and-spoofing/>

[112] Electronic Communications Committee, ECC Report 338 (7 June 2022), pp. 12–13, <https://docdb.cept.org/download/4027>

[113] Commsrisk, “Baltic Telcos Hail Blocks on Spoofed Inbound International Calls,” 7 June 2024, <https://commsrisk.com/baltic-telcos-hail-blocks-on-spoofed-inbound-international-calls/>

[114] https://wdocs-pub.chd.lu/docs/exped/2026/03/QP_62380_1772476961681.pdf

[115] Vanilla Telecoms, “Blocking of Calls to Protect Subscribers from Scam Calls,” 29 May 2024, <https://vanilla.net.mt/blog/blocking-calls-protect-scam-calls>

[116] Simon Woodhead, “Norway CLI Restrictions,” Simwood, 31 August 2022, <https://simwood.com/2022/08/norway-cli-restrictions/>

[117] Laurence Nivot, “National measures against spoofing practices in Europe,” Cullen International, 18 June 2024, <https://www.cullen-international.com/news/2024/06/National-measures-against-spoofing-practices-in-Europe.html>

[118] Vlad Constantinescu, “Romanian Telecom Firms Told to Block Foreign Calls Spoofing Local Numbers,” Bitdefender, 14 July 2025, <https://www.bitdefender.com/en-us/blog/hotforsecurity/romanian-telecom-firms-told-to-block-foreign-calls-spoofing-local-numbers>

[119] Mariano Gonzalez-Cayuela, “Spain drafts new regulations to fight spam calls,” Hiya, 29 August 2024, <https://blog.hiya.com/spain-drafts-new-regulations-to-fight-spam-calls>

[120] Swedish Post and Telecommunications Authority, “Telephone scams (spoofing),” 7 October 2024, <https://pts.se/en/internet-and-telephony/sakerhet-och-skydd-av-uppgifter/telephone-scams-spoofing>

[121] Ofcom, “Tackling scam calls: Updating our CLI Guidance to expect providers to block more calls with spoofed numbers,” 29 July 2024, p. 33, <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-2-6-weeks/276698---further-action-to-tackle--scam-calls/associated-documents/statement-tackling-scam-calls.pdf>



The following European countries have telcos that execute the soft-block version of this control.

- Austria [122]
- France [123]
- Germany [124]
- Switzerland [125]

The following non-European countries also have telcos that implemented one or other version of this control.

- Australia [126]
- Bahrain
- Egypt
- Hong Kong
- Oman
- India [127]
- Saudi Arabia
- Singapore [128]
- Taiwan [129]
- the United Arab Emirates

In addition, Denmark is working towards the implementation of blocks on inbound international calls by legislating to change its interpretation of GDPR to permit the transfer of data between mobile operators necessary for roaming status checks [130][131]. Only a minority of EU countries have yet to make any progress towards following the advice in ECC Recommendation (23)03.

[122] Rundfunk und Telekom Regulierungs-GmbH (RTR), “Teilerfolg im Kampf gegen Spoofing,” 2025, https://www.rtr.at/TKP/aktuelles/publikationen/newsletter/newsletter_2025/RTR.Telekom.Post-Newsletter_01_2025/teilerfolg-im-kampf-gegen-spoofing_de.html

[123] Arcep, “Numbering Plan,” 2 December 2025, <https://en.arcep.fr/news/press-releases/view/n/numbering-plan-021225.html>

[124] Bundesnetzagentur, “Improved protection against telephone number manipulation as from 1 December,” 29 November 2022, https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2022/20221129_NumberManipulation.html

[125] ASUT, Swiss Telecommunications Association, Swiss TSP Anti-Spoofing Agreement Technical Specification, version 1.2 (2025), p. 3, <https://www.bakom.admin.ch/dam/en/sd-web/IBkjWsrL9Kz-/Swiss%20Anti-Spoofing%20Technical%20Specification%20-%20V1.2.pdf>

[126] Communications Alliance Ltd, Industry Code C661:2022 Reducing Scam Calls and Scam SMS (2022), cl. 4.2.5., <https://www.austelco.org.au/publication/c661/>

[127] Indian Ministry of Communications, “Union Minister Jyotiraditya M. Scindia launches ‘International Incoming Spoofed Calls Prevention System,’” 22 October 2024, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2067113®=3&lang=2>

[128] Infocomm Media Development Authority (IMDA), “As part of anti-scam measures, Telcos to introduce option for mobile subscribers to block calls from international numbers,” 4 January 2024, <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/opt-to-block-incoming-international-calls>

[129] Jennifer Creery, “Taiwan May Have Figured out a Way to Beat Phone Scammers,” Bloomberg Technology, 9 November 2023, <https://www.bloomberg.com/news/articles/2023-11-09/taiwan-may-have-figured-out-a-way-to-beat-phone-scammers>

[130] <https://meremobil.dk/2026/02/fupopkald-danske-numre-spoofing/>

[131] <https://www.computerworld.dk/art/294183/teleindustrien-dropper-amerikansk-loesning-mod-svindelsatser-paa-nordisk-loesning-mod-spoofing>

Australian telcos were among the first to implement this control. The importance of the control for protecting Australians was emphasised by Iñaki Berroeta, CEO of TPG, Australia's third-largest telco, in a speech made in April 2024:

- *"We do not believe Australian numbers should be used by operators to originate calls and route anonymous, dodgy, foreign contact centres to Australians using a local number they do not hold."*
- *"Many Australians have answered a call from an Australian fixed or mobile number, only to find out it was a scam call from overseas."*
- *"This behaviour must not be permitted to occur."*

Berroeta's concern was that the effectiveness of Australia's general prohibition against international calls that present a spoofed number had been undermined by communications providers that serve offshored call centres and by international wholesale carriers that continue to allow businesses to use Australian phone numbers to originate traffic. While there may be some market demand for the legitimate spoofing of business calls, the absence of KYC controls over who can spoof calls is abused by criminal call centres that are only pretending to serve legitimate businesses.

This control is rarely discussed and even more rarely proposed by telecoms industry associations tasked with devising solutions to global fraud because it is opposed by American business interests. The characteristics of the numbering system implemented in the USA would increase the cost of implementing this control relative to most other countries, though the significance of this additional cost is debatable given the overall losses to fraud and the amounts spent by American telcos on other anti-scam controls. Opposition to this control is a key driver of the USA's pursuit of more complex ways of authenticating domestic and international calls, and then backing those methods through international traceback.

Deliberately omitting the potential benefits of this control from calculations about how to tackle crime on a global level results in considerable skew of the cost-benefit assessment of other controls that receive more support from American businesses. By simply not mentioning the extent to which scam calls can be reduced through the blocking of inbound international calls that spoof domestic numbers, they inflate the potential benefits of more elaborate and costly methods that place far greater reliance on international cooperation to be effective.

Although there is considerable resistance from American business interests, there are independent American experts who advocate for the adoption of this control within the USA. A February 2026 submission to the FCC from the Stop Scams Alliance asked for the adoption of blocks on inbound international calls that spoof domestic numbers in a section entitled "Significant results in countries that block spoofed international calls". The submission to our survey from Tom Walker, an expert who spent 20 years investigating fraud on behalf AT&T and T-Mobile USA, ranks the blocking of inbound international calls that present a domestic CLI as a superior anti-spoofing technique to the US implementation of STIR/SHAKEN.



Proven effectiveness so far	10	As the most impactful of all the methods reviewed for this report, this control sets the benchmark for all others
Range of communication channels covered by the method	2	Only for dialled international voice calls, and only for landline calls unless a roaming status check has been implemented
Range of uses covered by the method	1	Anti-spoofing only, though the method also indicates which telcos are allowing domestic phone numbers to be abused
Market readiness	9	The method is widely in use already, though different countries may need to invest time and effort in implementing a roaming status check that works appropriately with the systems used by all the domestic mobile network operators
Anticipated cost of implementation	10	The cost of the necessary systems are low compared to other methods reviewed, and it eliminates costs relating to enforcement, tracing the origin of bad communications etc.
Style of traceback	N/A	
National security	No national security implications other than ensuring any central pool of roaming status data is properly secured; arguably this control also reduces the risk of cross-border denial-of-service attacks	
Score	32	

SMS SENDER ID REGISTRIES AND OTHER REGISTRIES BASED ON THE ORIGINATING ADDRESS OF AN A2P TEXT MESSAGE

Though not as widely implemented as blocking of inbound international voice calls that spoof domestic numbers, the use of SMS Sender ID registries has emerged as the most effective counterpart tactic for preventing crime that involves text messages which present the recipient with a deceptive address. While controls on inbound international calls identify mismatches based on the nationality of a phone number, Sender ID registries identify mismatches between the registered user of a specific Sender ID address and the actual party trying to use it. When a communications provider receives a message with a registered Sender ID that did not come from the registered user, the provider blocks the message.

Alphanumeric Sender IDs are used in conjunction with the bulk messaging services offered by many CPs in many countries. Examples of Sender IDs that will be familiar to EU residents include “AIB”, as used for one-time passcodes (OTPs) sent by Allied Irish Banks, “FINNAIR”, as used for customer notifications sent by the Finnish airline, and “DHL” for parcel notifications from the multinational delivery firm. Bulk messaging services are accessed by corporate customers through a computer interface rather than by typing messages into a handset because the goal is to send a high volume of repetitive messages, such as OTPs. The computerised nature of the interface for these services is reflected in the name given to them within the communications sector: Application-to-Person (A2P) services, as contrasted with the Person-to-Person (P2P) communications that ordinary phone users can originate. The alphabet characters used in Sender IDs mean recipients can instantly tell who has sent a message but they also increase the risk if the same Sender ID is reproduced by an unauthorised party.



Networks support alphanumeric Sender IDs for A2P SMS in approximately 85% of all countries per the advice that global cloud communications provider Twilio gives to its customers. If Sender IDs are not supported then the originating address for an A2P message must be a series of digits, which may be of the same length and format as ordinary phone numbers, or may be a special length, such as four-digit 'short codes', depending on the specifics of how messaging systems work in that country. We will only examine Sender ID registries in detail because they represent the most common example of anti-scam messaging registries worldwide. However, the same concept of registering A2P senders and registering the numeric addresses they use has also been implemented in some countries that do not support Sender IDs. Our research only identified Belgium and Hungary as EU countries where alphanumeric Sender IDs are not supported.

The distinction between A2P and P2P messaging is important because an anti-scam control for A2P messaging is not a control over all messaging, although some parties may try to exaggerate the scope of anti-scam controls over A2P channels by failing to distinguish between A2P and P2P channels. On the other hand, there are other ways to mitigate the abuse of P2P channels which would not be appropriate for A2P channels and which will not be covered by this report. For example, communication providers should force messages sent by consumers to display the phone number associated with the device that sent the message, and deny P2P users the ability to select a Sender ID instead. Communication providers can also set limits on the number of messages that each user sends P2P, as appropriate for a consumer-oriented service, to prevent the channel being misused by businesses and spammers. Criminals will tend to prefer to use A2P channels if they can, because the cost per message will be lower, there will not be a cap on how many messages they can send, and they can select a Sender ID with the intention of deceiving the recipient, perhaps by presenting the name of a reputable business without their knowledge.

Blocking messages which use deceptive Sender IDs is not a new practice. Many communications providers have formulated their own rules concerning messages Sender IDs they will block because they represent a risk to the public. For example, if a business wanted to send a lot of messages with "PACKAGE DELIVERY" as the Sender ID then a prudent CP would refuse because the Sender ID is too vague and too easily misused. National registries provide coordination that enhances controls to prevent scams by allowing reputable organisations to record which Sender IDs will be used by them, so that all CPs in the country can prevent the same Sender IDs being used by imposters.

Some countries have mandatory Sender ID registries while others operate voluntary Sender ID registries. In a country where registration is mandatory, a reputable organisation must identify itself and record which Sender IDs it will use for A2P messaging. Any message with a Sender ID that has not been registered will be blocked. In a country where registration is voluntary, reputable organisations are able to register themselves and the Sender IDs they use. If another entity tries to send messages using one of the registered Sender IDs then the message will be blocked, but if nobody has registered the Sender ID then the message will still be delivered. Mandatory registries are hence safer for the public because all Sender IDs have to be registered, thus making it clear who is responsible for each message with a Sender ID and creating the opportunity to vet all the senders of bulk messages and exclude those senders who do not follow the rules.



National Sender ID registries have been adopted by the following countries.

Table 7: Countries with National Sender ID Registries

Country	Name and Administrator	Mandatory or Voluntary	Comments
Australia	SMS Sender ID Register (ACMA) [132]	Mandatory	
Austria	Public alphanumeric Sender ID directory (RTR) [133]	Mandatory	Enforcement starts 1 October 2026
Finland	Protected SMS Sender ID register (Traficom) [134]	Voluntary	
France	AF2M sensitive OADC authorisation list (AF2M) [135]	Voluntary	
Hong Kong	SMS Sender Registration Scheme (OFCA) [136]	Voluntary	Registered IDs display a leading #
India	TCCCPR Distributed Ledger Header Register (TRAI; operator registrars)[137]	Mandatory	A federated system where CPs operate nodes per TRAI rules
Ireland	ComReg SMS Sender ID Registry (ComReg) [138]	Mandatory	
Italy	Registro degli Alias (AGCOM) [139]	Mandatory	
Netherlands	SMS Sender ID Register (COIN)[140]	Voluntary	
Poland	Register of SMS Sender IDs reserved for public entities (CSIRT NASK) [141]	Voluntary	The registry is only for public sector entities
Saudi Arabia	National local bulk-SMS sender-name management system (CST)[142] [143]	Mandatory	This system is federated across multiple operator databases

[132] <https://www.acma.gov.au/industry-rules-sms-sender-id-register>

[133] https://www.rtr.at/TKP/was_wir_tun/telekommunikation/anbieterservice/sms-regulierung/sms-regulierung.de.html

[134] <https://www.traficom.fi/en/telephone-and-broadband/numbers-issued-trafficom/protected-sms-sender-ids>

[135] <https://af2m.org/protection-des-oadc-sensibles/>

[136] <https://www.ofca.gov.hk/ssrs/en/>

[137] <https://trai.gov.in/tcccpr>

[138] <https://www.comreg.ie/senderid>

[139] <https://www.agcom.it/provvedimenti/delibera-12-23-cir>

[140] <https://coin.nl/nl/diensten/sms-sender-id-register>

[141] <https://www.gov.pl/web/baza-wiedzy/wystartowal-system-wymiany-informacji-o-smishingu>

[142] <https://www.cst.gov.sa/media-center/news/First-of-its-kind-to-regulate-services-in-the-Kingdom-CITC-Launches-the-Local-Bulk-SMS-Management-Sy>



Table 7 (cont.): Countries with National Sender ID Registries

Country	Name and Administrator	Mandatory or Voluntary	Comments
Singapore	Singapore SMS Sender ID Registry (SGNIC / IMDA) [144]	Mandatory	The registry also accepts numeric Sender IDs
Spain	Registro de Alias (CNMC)[145]	Mandatory	Spain previously had a voluntary registry; enforcement of the mandatory registry begins 15 September 2026
United Kingdom	SMS SenderID Protection Registry (MEF) [146]	Voluntary	
Vietnam	National System for Management of Brandnames (AIS) [147]	Mandatory	

National Sender ID registries have been adopted by the following countries. The best evidence for the effectiveness of Sender ID registries comes from Singapore, where there is more experience of its use because they were one of the first countries to introduce a register and then to mandate registration. The Singapore register first entered voluntary service in March 2022, and is credited by the Infocomm Media Development Authority (IMDA), the Singaporean communications regulator, with being the reason for a 64% fall in online scams instigated by SMS between Q4 2021 and Q2 2022 [148]. The register then became mandatory in January 2023, prompting a further 70% fall in scam SMS messages during the following three months [149].

Other registers have proven successful too. South Korea does not have alphanumeric Sender IDs, but their register of bulk SMS senders entered full operation on 1 June 2024, followed by a six-month transition period for existing SMS aggregators. Translated from the Korean as a 'Bulk Message Transmission Qualification Certification System', it registers the intermediary authorised to originate bulk A2P SMS, rather than reserving a sender label or telephone number to a brand [150]. The Korea Internet and Security Agency began publishing statistics about the effectiveness of the new registry in January 2025, following the completion of the transition period. Complaints from the public about spam SMS messages fell from over 3.9 million in January 2025 to less than 900,000 by June 2025 and have continued to fall since [151].

[144] <https://www.sgnic.sg/smsregistry/overview>

[145] <https://www.cnmc.es/sectores-que-regulamos/telecomunicaciones/registro-alias>

[146] <https://mobileecosystemforum.com/sms-senderid-protection-registry/>

[147] <https://english.luatvietnam.vn/decreed-no-91-2020-nd-cp-dated-august-14-2020-of-the-government-on-fighting-against-spam-text-messages-spam-emails-and-spam-calls-189003-doc1.html>

[148] <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2022/full-sms-sender-id-registration-to-be-required-by-january-2023>

[149] <https://www.mddi.gov.sg/newsroom/measure-to-protect-singaporeans-against-online-scams/>

[150] Korea Communications Commission, 'Launch of the bulk-message transmission qualification certification system', 3 June 2024, <https://www.kmcc.go.kr/user.do?boardId=1113&boardSeq=61644&mode=view&page=A05030000>

[151] Korea Internet & Security Agency, monthly disclosures of reports attributed to domestic bulk-message relay operators and resellers, January 2025-July 2026, <https://spam.kisa.or.kr/spam/na/ntt/selectNttList.do?bbsId=1081&mi=1201>



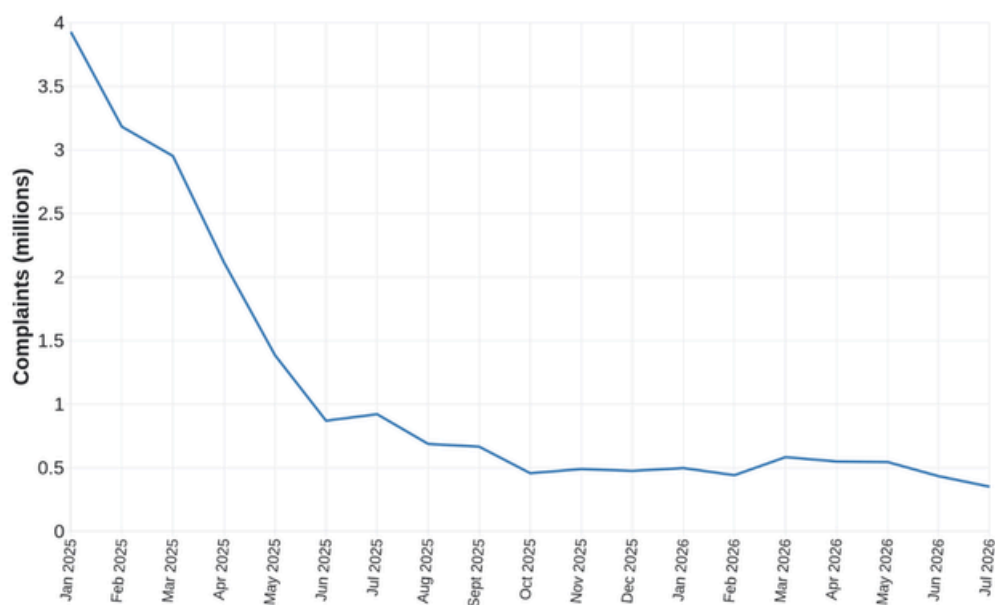


Figure 18: Monthly Spam Complaints Attributed to Domestic Bulk SMS Services in South Korea [152]

Proven effectiveness so far	9	Highly impactful
Range of communication channels covered by the method	2	Only for A2P messaging, and typically only for A2P SMS though the same concept can be applied to A2P RCS and other messaging protocols used by bulk senders
Range of uses covered by the method	2	Anti-spoofing only, though the method also helps to identifies bad actors among communications providers who try to facilitate unregistered messages
Market readiness	9	The method is widely in use already, though the specifics of how a register is maintained and enforced will vary from country to country and may need to be tailored to local circumstances
Anticipated cost of implementation	8	The cost of the registration systems are modest, though the need to accept, review and update registrations will be an ongoing overhead
Style of traceback	N/A, though the method can help to identify communications providers that violate anti-scam rules	
National security	No national security implications; arguably this control also reduces the risk of cross-border denial-of-service attacks	
Score	30	

[152] <https://spam.kisa.or.kr/spam/na/ntt/selectNttList.do?bbsId=1081&mi=1201>

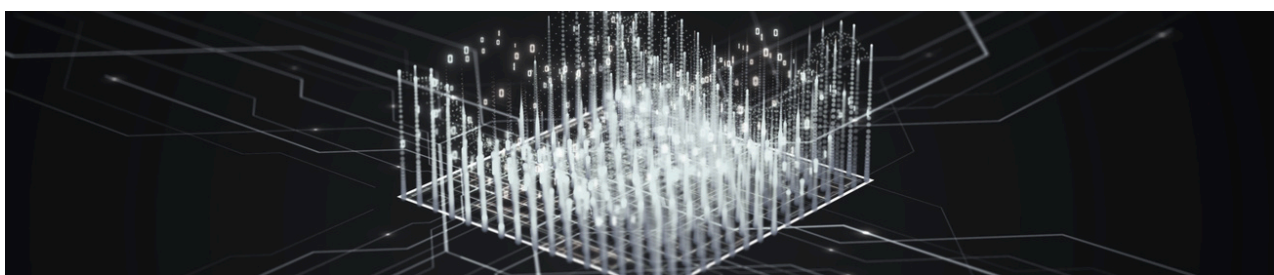


BLOCKING OF CALLS THAT SPOOF A PHONE NUMBER ON A NATIONAL DO-NOT-ORIGINATE (DNO) LIST

It would be difficult to find an expert in controls to mitigate telecoms fraud that would argue against the use of DNO lists. The principle is simple, and somewhat analogous to the use of SMS registries. Businesses and other reputable organisations need to publicise phone numbers that can be used to contact them. Criminals will sometimes impersonate those organisations by spoofing those same phone numbers when making an outbound call to their victims. The logic is straightforward; if the target questions whether the phone call is genuine, the scammer tells the victim to compare the CLI to the phone number that has been published by the organisation they are impersonating. So to prevent the number being abused in this fashion, a DNO register is maintained of numbers that reputable organisations only use to receive inbound calls, and never use to make outbound calls. If any call then presents a CLI that matches an entry in the DNO list then the communications provider knows they should block it because they can safely infer it has been spoofed by an unauthorised party.

Estimating the value of this control is impossible because it depends on the diligence of businesses that register their DNO numbers and the speed with which scammers abandon this deception when they begin to realise it has stopped working. In his submission to our survey, American telecoms fraud expert Tom Walker ranked the blocking of DNO numbers as the 'first line' of defence against fraudulent spoofed calls. Putting a value to the method is probably not necessary because the method is so simple, so cheap, and so effective at ending the abuse of numbers that well-known organisations use to receive calls that it is difficult to argue against its implementation. Even so, the quality of DNO lists do vary from nation to nation, and is influenced by how well the method is publicised to the businesses and other organisations that should register numbers they will only use to receive calls. When implemented well, a specific class of confidence trick is rapidly eliminated, forcing scammers to change their methods and rely upon presenting CLIs that are less likely to deceive potential victims.

Proven effectiveness so far	10	Highly impactful
Range of communication channels covered by the method	1	Only for voice calls and only for calls from organisations that have dedicated numbers for inbound calls only
Range of uses covered by the method	1	Anti-spoofing protection in relation to corporate entities with registered DNO numbers only
Market readiness	9	Many countries have DNO lists already; not much effort is required to educate new countries about how the method has been implemented elsewhere
Anticipated cost of implementation	9	The cost of the maintaining the DNO list and blocking calls that match DNO entries is low
Style of traceback	N/A	
National security	No national security implications	
Score	30	



BLOCKING OF CALLS THAT SPOOF AN INVALID, UNALLOCATED OR UNASSIGNED PHONE NUMBER

This group of anti-fraud controls is so simple and basic that many telcos in many countries have implemented versions of them already. It would be easy to exclude controls of this type from the review on the assumption that European communications providers already know how to implement these controls, and if they have not been motivated to implement them by now then they will never implement them. On the other hand, One Consortium did include this category of controls in its inventory of anti-scam methods, and the methods do relate to spoofing, a subject covered by this report. Reiterating the benefits associated with this control for this report's audience may result in telcos being reminded of the reasons to optimise controls of this type, especially because these controls are generally cheap and simple to implement.

The behaviour of scammers changes in response to anti-scam controls, but historically scammers have made extensive use of invalid, unallocated and unassigned phone numbers when spoofing the CLI of a voice call.

- **Invalid numbers:** a sequence of digits that cannot represent a legitimate phone number because it is inconsistent with the national dial plan of the country it supposedly relates to. Each national regulator imposes a dial plan for its country that stipulates how many digits are included in phone numbers and rules for how certain groups of digits relate to specific categories of phone users (for example, phone users in a specific geographic region, numbers associated with businesses where the cost of calling them is higher or lower than typical phone numbers, etc). Numbers are invalid if they are not consistent with the national dial plan because they contain too many digits, too few digits, or a sequence of digits that conflicts with the dial plan.
- **Unallocated numbers:** the national regulator has not given any telco permission to use this sequence of digits as a phone number. There are only finite permutations of digits consistent with a national dial plan, so regulators only give permission to use a subset of all the potential phone numbers. This allows them to efficiently manage their supply and discourage wasteful business practices. Numbers are usually allocated to telcos in 'blocks'; for example, a telco is allowed to use every number ending 8000 to 8999.
- **Unassigned numbers:** the telco has been allocated a number but has not granted use of that number to any customer. This is an inevitable consequence of numbers being allocated to telcos in blocks but then made available by telcos to their customers on a piecemeal basis.

It follows that there should never be any phone calls that present an invalid, unallocated or unassigned numbers as the CLI. However, historic data shows that scammers have often spoofed invalid, unallocated and unassigned numbers. Impersonation of a specific person or entity is not the goal when spoofing these numbers, but there are other types of deception that do not involve impersonation. For example, neighbour spoofing occurs when a scammer tries to increase the chances of their call being picked up because they present a CLI from the same geographic region as the recipient of the call, even the call originated somewhere else.



Estimates of the benefit to the public of blocking calls that spoof invalid, unallocated and unassigned numbers vary greatly, probably because the extent of related crimes will vary depending on whether telcos have already implemented controls to prevent them, the amount of profit that criminals can generate from calls based upon the current retail and wholesale tariffs for calls from one country to another, how much different national cultures are predisposed to trust or be suspicious of unfamiliar CLIs, and how well public awareness campaigns have trained the public to be suspicious. It proved impossible to find recent estimates in the public domain of the extent to which crime exploits invalid, unallocated and unassigned numbers for CLI of calls from fraudsters so we contacted an expert in the field to obtain his opinion. Guy Howie is the owner of Business Intelligence and Assurance Solutions Limited (BIAAS), a company that has supplied telcos with international number range intelligence and investigated phone numbers used by fraudsters for 20 years. His estimate was that investigations he conducts on behalf of clients typically involve between 10% and 30% of inbound voice calls from numbers that can be shown to be invalid or unallocated.

Controls to block inbound calls from invalid numbers are relatively simple to implement; they mostly require telcos to have sources of intelligence that keep them apprised of any changes to foreign dial plans that change which numbers are valid or invalid. Controls to block inbound calls from unallocated numbers are also simple to implement; this depends on intelligence about which numbers have been allocated in each country. Telcos can look up this information from resources published by the national telecoms regulators of each country, but most choose to outsource this task to a supplier of intelligence that constantly reviews worldwide number allocations on their behalf. In contrast, obtaining intelligence about unassigned numbers is much harder. Various countries have proposed the introduction of data sharing arrangements so that domestic telcos know which numbers have been allocated and which remain unallocated, but there has been little progress beyond the concept stage because the potential benefits are harder to estimate.

One slight variation of this control involves permitting inbound calls to be connected but then blocking any attempts by customers to make outbound calls to these numbers. The logic is that the receiving telco can charge a fee for the receipt of the call but will prevent any harm to customers by preventing anyone from dialling the number back.

Proven effectiveness so far	7	Though it is difficult to obtain expert estimates
Range of communication channels covered by the method	2	Only for voice calls
Range of uses covered by the method	4	Reduces the number of spoofed calls and the same intelligence can help telcos to manage costs and detect other ways that businesses are exploiting weaknesses in the telco's fee structure
Market readiness	7	The method is widely in use already for invalid and unallocated numbers, but there has been little progress for unassigned numbers
Anticipated cost of implementation	9	There is a degree of competition between suppliers of number range intelligence and telcos will likely already have firewalls that can be configured to block calls with matching numbers
Style of traceback	N/A, though the method can help to identify communications providers that collude with crime	
National security	No national security implications	
Score	29	

STIR, SHAKEN, RCD AND VESPER

STIR/SHAKEN, as it is widely but imprecisely called, refers to a collection of technology and governance protocols. Their purpose has, at different times, been said to be the authentication of CLIs of voice calls carried over IP networks or the traceback of communications. When the Pallone-Thune TRACED Act [153] passed into American law on 30 December 2019, it started a chain of events that would inevitably lead the USA to lobby for the global adoption of STIR/SHAKEN for CLI authentication and traceback. This has recently been reinforced by the US Senate approving the Foreign Robocall Elimination Act [154]. If the Foreign Robocall Elimination Act becomes law, as appears likely given the lack of opposition from either of the main political parties in the USA, it will explicitly call for the lobbying of foreign countries to implement STIR/SHAKEN by convening a task force comprising the same government and business interests that pursued the mandate of STIR/SHAKEN for US businesses.

Other countries are not devising anti-scam strategies involving CLI authentication and traceback in a vacuum. They are responding to this American initiative, sometimes by adopting STIR/SHAKEN (France), and sometimes by rejecting it (the United Kingdom). But when countries reject STIR/SHAKEN, the phrasing of the decision is usually couched to permit a reversal of that decision at a later date. This is important context for the commissioning of this report. When published, most eyeballs will focus on this chapter.

To be precise, this chapter concerns combinations of the following protocols.

- STIR, as defined by IETF RFCs 8224 [155], 8225 [156] and 8226 [157], published in February 2018
- SHAKEN, as defined by ATIS standard 1000074 [158], published in January 2017, and IETF RFC 8588 [159], published in May 2019
- SHAKEN governance model and certificate management, as defined by ATIS standard 1000080 [160], published in July 2017
- Rich Call Data (RCD), as defined by IETF RTCs 9795 [161] and 9796 [162] published in July 2025
- RCD under SHAKEN, as defined by ATIS standard 1000094 [163], published in April 2021
- VESPER, a draft IETF standard (draft-wendt-stir-vesper-00 [164]), with the first draft dated June 2024
- VESPER evidence for right-to-use (draft-wendt-stir-vesper-07 [165]), another draft IETF standard, with the first draft dated March 2026

[153] <https://www.congress.gov/bill/116th-congress/senate-bill/151/text>

[154] <https://www.congress.gov/bill/119th-congress/senate-bill/2666/text>

[155] <https://www.rfc-editor.org/rfc/rfc8224.html>

[156] <https://www.rfc-editor.org/rfc/rfc8225.html>

[157] <https://www.rfc-editor.org/rfc/rfc8226.html>

[158] https://access.atis.org/apps/group_public/download.php/67436/ATIS-1000074.v003.pdf

[159] <https://www.rfc-editor.org/rfc/rfc8588.html>

[160] <https://cdn.atis.org/sti-ga.atis.org/2026/03/31143346/ATIS-1000080.v006.pdf>

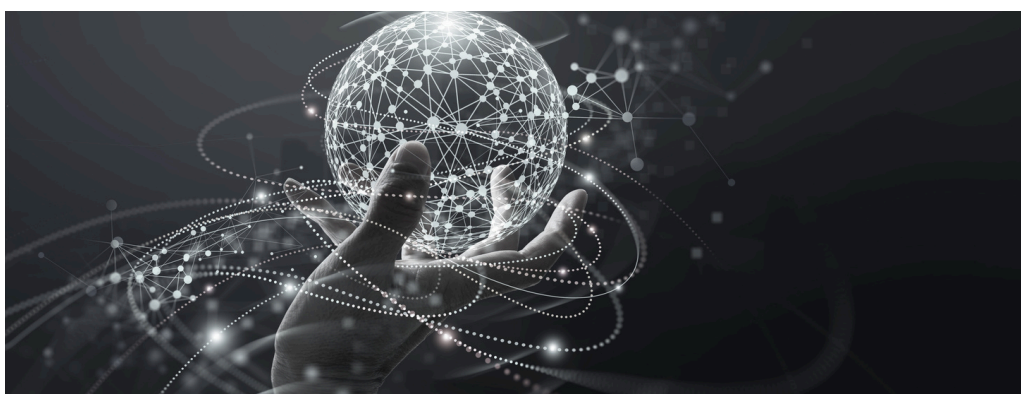
[161] <https://www.rfc-editor.org/rfc/rfc9795.html>

[162] <https://www.rfc-editor.org/rfc/rfc9796.html>

[163] <https://access.atis.org/higherlogic/ws/public/download/58888/ATIS-1000094.pdf>

[164] <https://www.ietf.org/archive/id/draft-wendt-stir-vesper-00.html>

[165] <https://www.ietf.org/archive/id/draft-wendt-stir-vesper-07.html>



With so many separate definitions of the components that may or may not be included in a specific implementation of ‘STIR/SHAKEN’, it is not surprising that most people talk loosely about STIR/SHAKEN as if it is a single homogenous system rather than articulating which specific elements have or have not been realised in practice. This creates a risk for this review. An international framework for authentication and traceback will require compatibility of systems implemented in different countries. The compatibility of STIR/SHAKEN implementations cannot be assumed just because two countries both use the term ‘STIR/SHAKEN’ to label the systems they have implemented. This has already been shown in practice, with France’s version of STIR/SHAKEN being incompatible with the versions implemented in the USA and Canada.

An astute reader can already infer that STIR/SHAKEN is by far the most fully developed series of protocols of its type. No other protocols that promise to offer similar capability to trace or authenticate dialled voice calls have received anything like the investment of time and resources that have been poured into STIR/SHAKEN. None have been tested in real life like STIR/SHAKEN has been tested in real life. However, that does not mean STIR/SHAKEN has delivered on its promises. On the contrary, the effectiveness of STIR/SHAKEN has been routinely exaggerated by its proponents, with the political support that comes from the protocols being mandated by law. The absence of currently viable like-for-like alternatives to STIR/SHAKEN should not be confused with the hope that STIR/SHAKEN is an effective way to reduce crime in practice. On the contrary, the content of later specifications being added to the STIR/SHAKEN ‘family’, such as VESPER, shows how weaknesses of STIR/SHAKEN that receive little attention still continue to be addressed by the businesses which supply the technology, over six years after they persuaded the US government that it was ready for use.

The purpose of VESPER, which is a working draft instead of an approved standard, is to establish whether the A-party that makes an outbound call has the right to use (RTU) the number that will be shown to the recipient of the call. Most non-specialist audiences wrongly assume this concept was inherent to the ‘authentication’ promised by STIR/SHAKEN years earlier. In other words, the purpose of VESPER is to stop impersonation fraud by preventing somebody choosing a CLI for their outbound calls that they are not authorised to use.

There are so many gaps between the claims made publicly about STIR/SHAKEN and what the protocols can realistically deliver in practice that it would be impractical to document them all here. For brevity, we will concentrate on the most important shortcomings of STIR/SHAKEN. The need for an additional protocol like VESPER has not been well appreciated by non-technical audiences but can be sufficiently established by anyone who reads the VESPER drafts. The other especially obvious shortcoming that some audiences still fail to appreciate is that some of the implementations of so-called STIR/SHAKEN are actually implementations of SHAKEN without STIR. For STIR/SHAKEN to be effective globally, given the current state of networks around the world, would also require the widespread realisation of SHAKEN without STIR.

STIR only works on IP networks. Many voice calls continue to be carried by other networks for some or all of the route from origin to destination. The data defined by SHAKEN can only be used to authenticate the originator of a call, or to trace a call back to its origin, if that data is successfully conveyed end-to-end from the origin to the destination. So if SHAKEN is only used in conjunction with STIR, then the objective of SHAKEN is failed every time the actual call path traverses a non-IP network.



The imprecise use of the phrase 'STIR/SHAKEN' means it is sometimes applied to scenarios where SHAKEN is implemented without STIR. This limitation has always been understood by the proponents of STIR/SHAKEN, though they typically understate the negative implications for law enforcement and consumers. The USA has only made extremely limited progress with implementing SHAKEN in the absence of STIR, despite significant amounts of domestic voice traffic being carried over routes that do not support STIR. The coherence of US arguments for the universal adoption of SHAKEN is undermined by the slow progress being made towards comprehensive adoption of SHAKEN within the USA.

Industry insiders will be fully aware of the anomaly created by the USA mandating STIR/SHAKEN for IP networks while failing to mandate SHAKEN for other networks. Proponents of SHAKEN have long understood the need for 'out-of-band SHAKEN', a mechanism that would allow SHAKEN data to be transferred between telcos in the absence of the in-band SIP signals supported by IP networks. Out-of-band SHAKEN is also intimately tied to the notion of 'International SHAKEN', because of the realisation that the USA cannot simply mandate the replacement of TDM networks with IP networks everywhere on the planet.

The likeliest explanations for the limited interest in realising out-of-band SHAKEN within the USA is that the current prices for carrying voice traffic within the USA incentivises some carriers to maintain existing TDM technology where it is more profitable, and that the out-of-band transfer of data may be less effective at supporting the transfer of supplementary data for which telcos can charge businesses a premium, such as RCD. When looked at purely from the perspective of law enforcement, out-of-band SHAKEN would be more advantageous than STIR/SHAKEN, because it could be realised universally today, irrespective of whether telcos operate IP or TDM networks. However, to avoid further confusion we will now separate into the next review our discussion of the potential for out of band SHAKEN and out of band VESPER to be realised separately from STIR.

With this in mind, it is worth noting that the pursuit of STIR/SHAKEN as a universal system that would be applied to all dialled voice calls ignores the reality of progress in implementing STIR/SHAKEN within the USA. STIR cannot be used in conjunction with older networks based on TDM technology. Predictions for how soon countries will transition to exclusively using IP networks have tended to be overly optimistic. Norway has already completed its transition to all-IP networks. Spain has made substantial progress towards completing the goal. The UK is set to complete the transition by January 2027. France and Italy are expected to complete their transitions around 2030. The FCC is proposing to remove mandates for the maintenance of legacy TDM in the USA by the end of 2028. Germany and Switzerland are unlikely to complete their transitions to all-IP networks before 2035. For other European countries, it is hard to predict when they transition to exclusively IP networks for carrying voice calls.

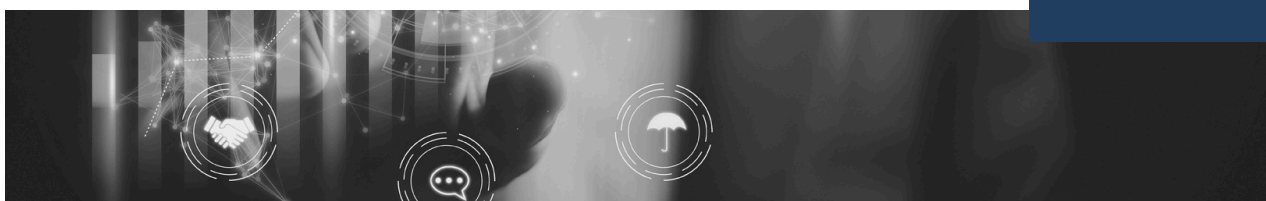
However, it is misleading to concentrate on the dates for transition discussed by rich countries, or to treat the dates as driven by regulatory intervention. When discussing traceback in a global context, the issue will be whether interoperable systems are implemented by both the rich countries where the largest number of consumers will complain about scams, the other countries which house scam call centres and all the intermediate countries that also need to support traceback. Many network operators in poorer countries will rapidly replace TDM with IP networks because of the substantial cost savings they will enjoy as a result. Overall, regulatory intervention is as likely to delay the transition to IP networks as accelerating it. This is because some national regulators intervene in the pricing of services supplied between telcos in ways that protect the interests of telcos with older infrastructure. The USA and Canada are examples of countries where the pricing of traffic disincentivises the replacement of some TDM network infrastructure. This is somewhat ironic given that the national regulators of in both countries also extol the benefits of STIR/SHAKEN.

Similar conflicts of interest will occur in other countries. It is not hard to imagine scenarios where government agencies superficially appear to be cooperating with the international goal of reducing crime through traceback but delay the transition to IP networks because they wish to stymie law enforcement. The income generated by scams is large enough to give some governments a reason to actively thwart the success of international traceback by keeping TDM networks in service. They may not even be seeking to protect criminals in their own country. If criminals run scam compounds in a third country, then telcos in an intermediate country will benefit from the income generated by traffic that has been deliberately routed through their TDM networks in order to defeat traceback requests from the country where the victims live.

Given all of the above, it should be clear that STIR/SHAKEN will never be an effective foundation for a global tracing system. Even if the EU was to copy the mandate imposed in the USA, by mandating STIR/SHAKEN for all IP networks within its borders, the approach would still be rendered ineffective for tracing calls that begin and end in the EU because of the slow rate of transition to IP networks in some EU countries. And this weakness comes before the even more challenging prospect that calls which originate and terminate in the EU could simply be routed by criminals through countries outside of the EU in order to defeat the EU's tracing systems. Tracing systems that have to work hop-by-hop, because they must utilise the same in-band routes as the communication being traced, are intrinsically unsuited to the objective of tracing international communications in a world where no single authority can impose the same technologies and the same laws across all networks capable of carrying dialled voice calls.

Criminals can selectively route calls to ensure they are conveyed by networks that do not support STIR, and hence do not support traceback using the combination of SHAKEN with STIR. Even a high degree of STIR/SHAKEN coverage is irrelevant if there are routes that criminals can use to bypass it. But as noted above, advanced criminals are already transitioning to using other communication channels instead of dialled voice calls. A traceback system that only traces traditional dialled voice calls will take years to implement, and will require even more years before it becomes fully comprehensive. Such a system is likely to be redundant long before its coverage is complete because scammers will have stopped using dialled voice calls in the meantime, and will accelerate the transition to OCS voice and other communications channels if the roll-out of STIR/SHAKEN is accelerated.

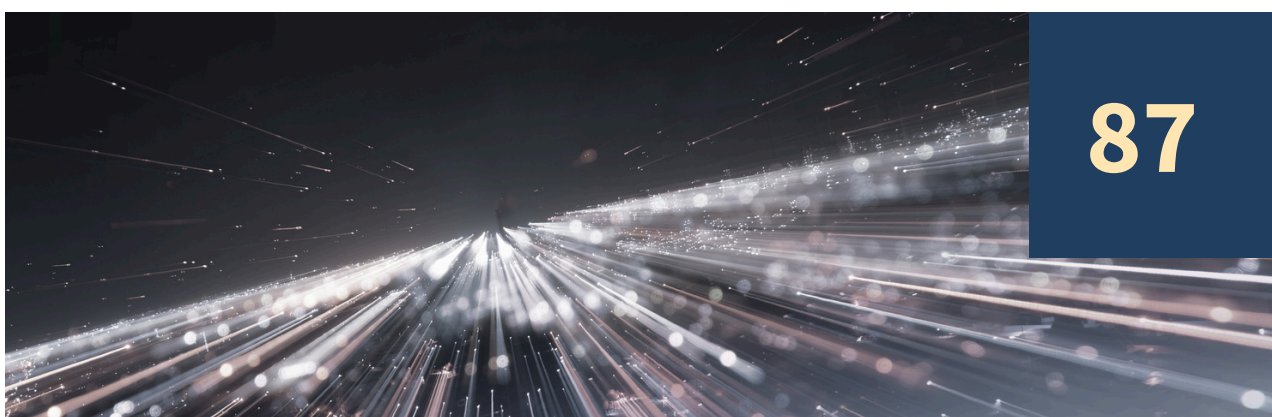
The suitability of STIR/SHAKEN for authenticating traffic is more debatable. If the goal is to provide additional assurance that legitimate voice calls are legitimate, then it can be argued it will be effective for a lot of voice traffic. If the goal is to eliminate the risk of harmful traffic by requiring all traffic to be authenticated, then the objective is unrealistic. Many of the statistics that advocates of STIR/SHAKEN present when claiming it has benefited American consumers concentrate on ideal scenarios that are less prone to crime anyway. For example, a very high proportion of traffic sent from mobile phone customers of Verizon to mobile phone customers of AT&T will arrive with an intact A-grade SHAKEN signature, indicating the CLI shown on the recipient's screen is consistent with the phone number of the person who dialled them. But organised crime syndicates are not going to originate lots of illegal traffic between Verizon and AT&T unless they are obtaining SIM cards in bulk with the intention of using them for a short period and then enduring the cost of the SIM cards and associated equipment being seized on a periodic basis. Many of the calls being traced in the USA appear to be of this nature, but there has not been many prosecutions, presumably because law enforcement agencies do not want to devote resources to finding who obtained the SIM cards and set up the equipment, and because they are not sufficiently aided by the KYC checks and records of the telcos that supplied the SIM cards.



The more realistic crime-reduction incentive for adopting the STIR/SHAKEN family of protocols within the USA is that it will reduce the liabilities of large enterprises by making it less likely that members of the public will be duped into believing they are receiving calls from big brand name entities such as Amazon or Microsoft. The RCD protocol enables the carrying of additional data alongside SHAKEN. A recipient of a call with RCD data will be shown the logo of the company that calls them, and an explanation for why they are being called. This is expected to increase the chances of consumers accepting the call. When its use becomes widespread, it also means that recipients of calls will be less likely to be tricked by calls from sources that impersonate big brands but which cannot utilise RCD functionality. This will reduce certain kinds of impersonation fraud for those big brand entities that choose to pay the premium charges that will be levied by telcos for carrying RCD data across their SIP signalling networks.

Whether the proposition of safer big brand calls is appealing to the EU will depend on attitudes towards services being supplied from foreign call centres and the answers to questions about who ultimately governs the use of a cross-border authentication system. Big brand businesses operate in the EU too, and fraudsters try to impersonate them. However, the impersonation of a business through a business call is less of a risk if consumers never receive calls from businesses. Stricter prohibitions over calls by businesses to consumers in some European countries means consumers are better able to identify scam calls. Fewer business calls means there is also less potential profit to be made by charging a premium for services like RCD. And even if services like these were introduced, it would raise political questions about fair competition. Will there be intervention in the market to ensure the cost of branded calling is kept low enough to not create an unfair advantage for big businesses over their smaller rivals? What if American multinationals make more use of branded calling to reach potential customers inside the EU than their European competitors? And who governs access to branded calling so that businesses which abuse the service when making international calls are subjected to the same punishments irrespective of which EU they are based in, or if they are based in the USA or another country outside of the EU?

The history of enforcement of GDPR shows consistent application of consumer protection rules is difficult to effect across multiple jurisdictions, even if all the jurisdictions are within the EU, and then becomes even more difficult to effect when dealing with businesses based outside of the EU. In the worst case scenario, a transnational governance body could negatively affect EU businesses by making it harder for them to obtain branded calling, or by more strictly enforcing consumer protection obligations for those businesses than for competitors based outside of the EU. The ultimate sanction in a transnational governance ecosystem would involve denying a communications business the right to apply SHAKEN signatures to calls, effectively barring them from making calls to countries that insist on SHAKEN signatures for the calls they receive. These questions fall outside the remit of this report, but they do influence the cost-benefit calculations for whether the STIR-SHAKEN-RCD-VESPER family of protocols are suitable for the EU.



Proven effectiveness so far	5	The actual performance of STIR/SHAKEN in the USA is significantly below the levels that were promised
Range of communication channels covered by the method	2	Only for voice calls and only when conveyed end-to-end by IP networks using SIP signalling
Range of uses covered by the method	8	The method can theoretically be used for traceback as well as authentication if SIP is supported end-to-end, and the method also supports premium marketing services that help customers identify big brand businesses
Market readiness	9	There is a variety of suppliers for the more basic functionality of STIR/SHAKEN, and also competition to supply the more advanced services
Anticipated cost of implementation	0	The cost of implementation is high; communications providers will seek to levy additional fees from follow-on services to realise the value of their investment
Style of traceback	Hop-by-hop	
National security	The need for transnational governance over the supply of certificates and recognition of tokens gives rise to the potential misuse to erect trade barriers	
Score	24	

OUT OF BAND SHAKEN

In this review, we also cover the largely unrealised potential for out of band SHAKEN, as separate from the claims made for call authentication and traceback systems that involve SHAKEN and other data carried in-band across SIP networks. To be precise, this section concerns the official methods for transferring SHAKEN out of band, as described in ATIS standards 1000095 [166], 1000096 [167], 1000105 [168] and 1000107 [169][170]. There is no theoretical limit on how to transfer any data outside of a system, so some of the methods of transferring SHAKEN data that are not described in ATIS standards are also covered in the review of subsequent methods.

[166] https://access.atis.org/apps/group_public/download.php/67542/ATIS-1000095.v002.pdf

[167] https://access.atis.org/apps/group_public/download.php/60535/ATIS-1000096.pdf

[168] <https://access.atis.org/higherlogic/ws/public/download/79509/ATIS-1000105.pdf>

[169] <https://atis.org/press-releases/new-atis-standard-to-extend-shaken-caller-authentication-across-tdm-networks/>

[170] https://store.accuristech.com/standards/atis-1000107-v002?product_id=3125173



ATIS standards for the out of band transfer can be broken into two categories:

- How to transmit the SHAKEN data without conveying it through SIP signals. The standardised methods ultimately come down to a process where the data is written to Call Placement Service (CPS) by the upstream communications provider, and then is read from the CPS by a downstream communications provider. In effect, the upstream telco uploads data to a server accessible via the internet, and then the downstream telco discovers where the data has been uploaded, and collects the data from the server.
- How telcos that interconnect with each other using TDM 'agree' which CPS they will use while preserving the same hop-by-hop sequence for data transfer as inherent to conveying SHAKEN using STIR.

This begs a rather obvious question. If SHAKEN can successfully be transferred out of band using a CPS, why restrict the transfers so they are all hop-by-hop transfers between telcos that have interconnected with each other? Why not just use the CPS to transfer the data in a single hop from the originating telco to the terminating telco, thus eliminating the need for transfers via all the intermediaries? With respect to traceback, eliminating all the intermediaries reduces the risk that a trace is not completed because of the non-compliance of an intermediary. With respect to authentication, the risk of the authentication data being lost or corrupted during transit is eliminated.

This author has never heard a plausible explanation for the apparent opposition of some American businesses to skipping hops in the out of band transfer of SHAKEN. There is a repeated and perverse desire by some businesses to describe out of band SHAKEN as if it only exists to fill the gaps in a hop-by-hop approach. This leads to even more perverse descriptions of out of band SHAKEN as an extension of STIR/SHAKEN when it really consists in using SHAKEN in the absence of STIR. In all likelihood, opponents of a more direct transfer of SHAKEN between originating and terminating communications providers are using discussions about technology and the need to attain consensus in order to obfuscate decisions that are motivated by political or commercial objectives.

- The hop-by-hop transfer of data ensures all carriers responsible for conveying a call can potentially be held liable for not blocking it, even if there is no good reason for those businesses to block it. So even if it is not possible to trace a call to its origin, or to punish the people responsible for originating the call, a state may impose a penalty on intermediate carriers for not using another technique – such as 'reasonable analytics' or machine learning – to identify scams and block them.
- Telcos can charge users for the use of the SIP signalling performed by their networks just like they can charge for any use of any aspect of their networks. If data has to be transferred by SIP, or by an alternative method, through every telco in the chain from origin to destination, then every telco has an opportunity to levy a fee for their part in conveying the data. If the data was transmitted out of band through a process that skips intermediate telcos, they would have no opportunity to levy a fee.

The ATIS standards for out of band transfer of SHAKEN appear to be readily scalable and could be implemented across the EU or worldwide without all of the issues created by assuming a SIP infrastructure is (mostly) in place first. But anecdotal reports suggest there has only been trivial adoption of out of band SHAKEN in the USA so far.

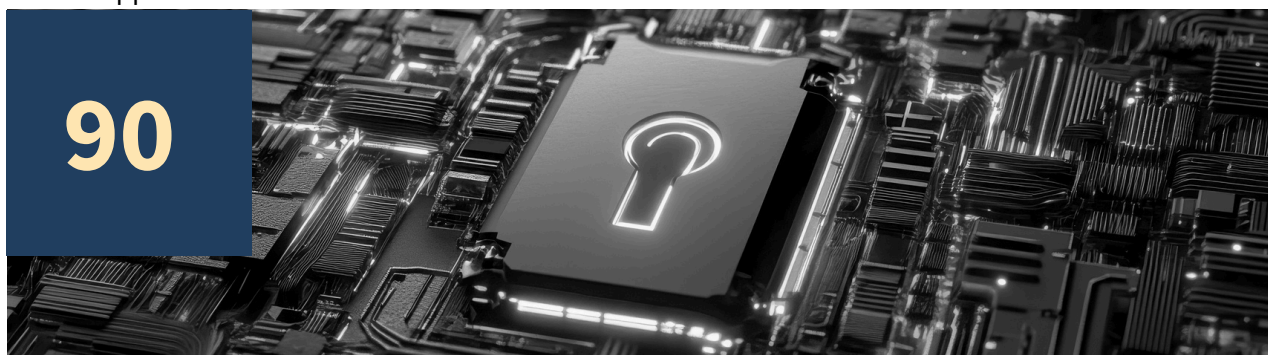


Rather than thinking of SHAKEN as an adjunct to STIR, the EU would be advised to run its own independent pilot studies on the potential mass adoption of SHAKEN through an out-of-band mechanism if the goal is the most rapid and most comprehensive form of authentication and traceback based upon the SHAKEN standards. This could be unpopular with businesses that would lose revenue generating opportunities as a result. However, it would also enable the direct form of traceback that eliminates the insurmountable flaws in the hop-by-hop international traceback strategy currently being promoted by American interests.

Proven effectiveness so far	4	The out of band SHAKEN standards exist and have been the subject of considerable expert work but there are limited examples of them being implemented in practice
Range of communication channels covered by the method	6	Decoupling SHAKEN from STIR gives rise to the theoretical prospect of SHAKEN or SHAKEN-like tokens being used for the tracing and authentication of different communication channels than dialled voice calls
Range of uses covered by the method	7	The uses of SHAKEN without STIR are the same as the uses of SHAKEN with STIR, except that the abandonment of hop-by-hop data transfers would alter which communications providers are covered
Market readiness	7	There are several businesses which offer relevant out of band SHAKEN services though their experience may be limited due to a lack of demand so far
Anticipated cost of implementation	5	a direct form of out of band SHAKEN transfer would eliminate all the costs involved in transferring the data through intermediaries
Style of traceback	Direct or hop-by-hop depending on how the SHAKEN data is routed	
National security	The need for transnational governance over the supply of certificates and recognition of tokens still gives rise to the potential misuse to erect trade barriers	
Score	29	

ORIGEM VERIFICADA

Most of our review has concerned the style of STIR/SHAKEN technologies implemented in the USA and Canada, as developed and supplied by North American businesses and mandated by the authorities in each country. There are also mature deployments of STIR/SHAKEN on a national scale within France and Brazil. This review concerns the Brazilian adaptation of STIR/SHAKEN, entitled ‘Origem Verificada’ and implemented by Cleartech. Cleartech is one of the businesses that responded to our survey and we consequently engaged in follow-up conversations with a view to confirming some details of how they adapted STIR/SHAKEN. However, we will first put the Brazilian approach into context by discussing the French approach.



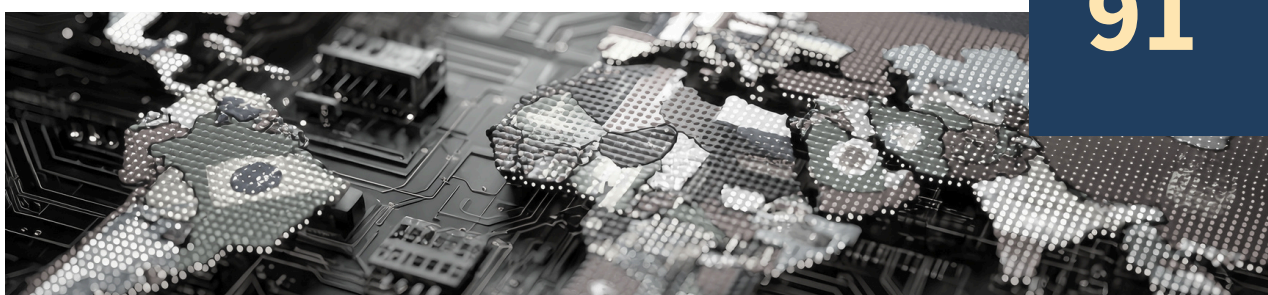
France's approach to STIR/SHAKEN, entitled Mécanisme d'Authentification des Numéros (MAN), is too similar to that in North America to merit a separate analysis. MAN simplifies the governance by eliminating some layers of bureaucracy. MAN also involves tokens which are not interoperable with those in the USA. Most importantly, the simplification in bureaucracy creates a national centralisation of control that simplifies execution in one country but complicates questions about how their systems would share governance for international calls; the question is somewhat analogous to how a central currency is governed when used across multiple countries because the policies adopted could unfairly favour businesses in one country over businesses in other countries. The US governance structures, while elaborate, are clearly better structured for potential internationalisation, while still begging questions of whether transnational governance bodies really would be neutral in their application of policy. But apart from this digression, the French differences with North American STIR/SHAKEN do not deserve further analysis. In contrast, some aspects of Brazil's Origem Verificada, deserve to be articulated in this report. They raise the prospect of a more cost-effective way of delivering similar results because Brazil uses an out-of-band method of data exchange not described by the official ATIS standards.

Brazil's approach to authentication is focused on business-to-consumer calls because the country has a culture where telesales and telemarketing is more common and more legally permissible than other countries. This has led to a high volume of complaints from consumers about abusive business practices. Brazilian authorities are less concerned about scams originating abroad. Like France, Brazil has reduced the number of bureaucratic layers in managing its version of STIR/SHAKEN by merging the separate American roles of a single policy administrator and multiple certification authorities. This merger also lends itself to a simple but effective way of transmitting SHAKEN data out of band. Instead of concerning themselves with hop-by-hop transfers, the terminating telco can obtain the SHAKEN data needed to authenticate a call and to present relevant RCD data to the recipient of a call by using the REST API of the central system.

The technology of REST APIs is well known and cheap. It is effective in practice. There is no reason to believe the methods used in Brazil, while not formally specified anywhere, could not be reproduced in the EU or elsewhere.

The current architecture of Origem Verificada is concerned with the authentication of domestic calls only; it is not suited to international traffic, though further adaptations would also be possible. As in France, any centralised national structure gives rise to questions about governance when handling communications that cross international borders. But the use of REST APIs to transfer authentication and traceback data is an innovation that deserves further examination if the EU intends to create a continent-wide system. A system exploiting REST APIs to transfer data out of bounds would likely be cheaper and quicker to deliver, while sidestepping some of the obstacles created by assuming TDM networks need to be replaced to get comprehensive international coverage.

The use of REST APIs positions Origem Verificada as a kind of halfway house between the standardised version of STIR/SHAKEN implemented in the USA and the non-standard national exchanges of CP data implemented in countries like Poland. It may hence be worth examining as a potential model for integrating national data exchanges with each other over time through the standardisation of some elements of the data transfer.



Proven effectiveness so far	9	Origem Verificada has more limited ambition than other major deployments of STIR/SHAKEN but reports from the authorities and the press suggest it has been highly effective at meeting the stated objectives
Range of communication channels covered by the method	1	Origem Verificada only applies to business-to-consumer voice calls, though the REST API adaptation could have broader application
Range of uses covered by the method	1	The system only exists to reassure Brazilian customers about calls from corporate entities
Market readiness	10	The system is stable and working
Anticipated cost of implementation	8	Brazil's approach was guided by a need to keep costs low and avoid changes to Brazilian networks
Style of traceback	Direct, in the sense that the central authority will know which businesses were responsible for the outbound calls received by consumers	
National security	The architecture of centralised national systems raises questions when trying to adapt them for international traffic	
Score	29	

OCULEUS 2FN (PREVIOUSLY KNOWN AS GSMA CALL CHECK)

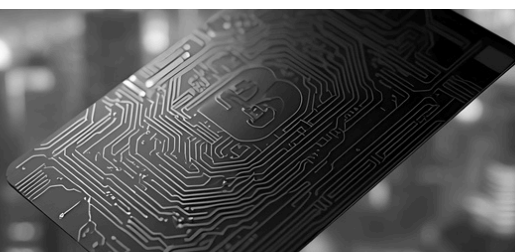
Oculus Two Factor Network (2FN) is a prototype for a universal out-of-band method for authenticating and directly tracing communications that was specified by the GSMA and developed by a German telecoms software business, Oculus GmbH. It is the subject of several patent applications [171][172][173]. The method was designed to minimise the implementation and operating costs of controls that protect consumers from scams and protect communications providers from fraud while maximising the immediate potential range of worldwide deployment by using software nodes that run in the cloud and communicate with each other using APIs.

Per the original design, each telco would have its own node and the nodes would exchange intelligence with each other. As a consequence, CPs would not need to make any changes to their networks or other systems in order to join a growing intelligence-sharing matrix. The GSMA had the exclusive rights to market and sell the system, which they branded as GSMA Call Check. The GSMA would also act as the ultimate governance authority by deciding who could use Call Check. However, interest from the mobile network operators that belong to the GSMA was disappointing. Telcos that took an initial interest cited an inherent problem with any proposition whose popularity depends on network effects: there is no incentive to join an intelligence-sharing matrix until others have already joined. The GSMA consequently abandoned their sales and marketing rights, which reverted to the developer. The product remains available and has been integrated with other anti-fraud products supplied by Oculus, but the intelligence-sharing matrix is unlikely to gain significant traction in the market unless one or more nations back it with a US-style mandate for authentication and traceback.

[171] <https://patents.google.com/patent/DE202023106573U1/en>

[172] <https://patents.google.com/patent/WO2025098549A1/en>

[173] <https://patents.google.com/patent/WO2025098573A1/en>



There is not much to say about the details of how the system works in practice because it is both a prototype and is also very simple. Communications are authenticated by the originating party informing its 2FN node of the outbound communication, and this information is then encrypted and securely transmitted over the internet to the node of the receiving party. If a communication between two telcos has been manipulated by an intermediary party, such as a change to the CLI of a call, or the altering of the originating number associated with a P2P SMS, this will be apparent to the terminating communications provider because of a mismatch with the data it receives at its 2FN node.

Other kinds of mismatches would indicate other kinds of fraud, such as charges for the delivery of an SMS that has not actually been delivered, or the manipulation of the apparent duration of a call to increase the amount charged for it. Direct tracing is possible if the receiving party retains a copy of the data that proves where the communication originated. Roaming status checks are possible if mobile operators within the same country use the nodes to query each other about the roaming status of their customers. Such roaming status checks would support the implementation of ECC Recommendation (23)03 for mobile phone numbers.

As the 2FN method is entirely based upon nodes running in cloud containers, it could be applied to any form of electronic communication, such as over the top messaging and voice services, although this has not been tested in practice. All that is theoretically required is that the originating and terminating businesses both have 2FN nodes and both choose to allow the exchange of data between those nodes.

Independent testing has been performed to ensure the system complies with European norms for security and privacy. This was conducted by a leading German telecoms security consultancy, SR Labs. The GSMA also assured themselves that the product would meet European security and privacy expectations. The method is inherently private-by-design because the nodes do not retain any data after it has been exchanged and there is no central store of data. The decentralised nature of the system means it does not introduce the national security risks inherent to systems with a centralised architecture. It was believed this would make the system more appealing in markets concerned with data sovereignty.

Considerable potential does not mean anything unless a system can be shown to work at scale. However, if the EU is to reject proposals for an American-style system for authentication and tracing, then 2FN would offer a credible alternative vision for how to meet the objectives of EU law enforcement agencies.



Proven effectiveness so far	4	The system has been tested but not subjected to deployment at scale
Range of communication channels covered by the method	10	The method is theoretically applicable to any form of electronic communication
Range of uses covered by the method	10	As a general-purpose system for exchanging information in real-time, it can be used for a wide range of purposes as well as authentication and traceback; the practical limit depends on the speed at which nodes process and communicate data because of the data centre resources that support them
Market readiness	2	The method has been on the market since late 2024 but there is limited experience of deploying it in practice and the developer is too small to accept many new customers at the same time without obtaining a larger business partner or franchising its technology
Anticipated cost of implementation	9	The simplicity of the system makes it one of the cheapest included in this review
Style of traceback	Direct, but dependent on either terminating parties maintaining records of which communications were authenticated, or on the system being adapted so law enforcement agencies obtain a node which receives a copy of data sent to communications providers within their country	
National security	No risks identified	
Score	35	

CHAKEN

Per the content of Chinese National Standard GB/T 43779-2024 [174], CHAKEN has been developed with the assistance of two of the three largest manufacturers of handsets in the world, Samsung and Xiaomi, as well as input from China's network manufacturers, telcos and academics. That alone is sufficient to demand a level of attention. The CHAKEN standard promises a significant upgrade to the capabilities of STIR/SHAKEN, extending the core principles so that authentication is transmitted from the originating user's handset to the recipient user's handset, not just from CP to CP. An approach like this is more in keeping with Europe's eIDAS roadmap, which places greater emphasis on consumers retaining control of how their own identity is used rather than renting the use of their identity from a centralised supplier or industry consortium.

CHAKEN also takes the presentational ideas instantiated in RCD and elaborates them significantly. Instead of just presenting a still image that represents an incoming caller, such as their corporate logo, the receiving handset will play a video recorded by the A-party. But the most exciting promise made by CHAKEN is that the technology would not be limited to the corporate market served by RCD. Any phone user would have access to the full range of identification and authentication features of CHAKEN. So instead of just tackling the impersonation of big brand entities, CHAKEN would reduce the risk of anybody being impersonated by a phone call. This is a tantalising prospect in an era where there are genuine concerns that deepfakes can be used to replicate how somebody sounds.

[174] <https://openstd.samr.gov.cn/bzgk/std/newGblInfo?hcn=E23E1CA2CB5848D103B39C4C95700CCB>



However, there is no convincing evidence that CHAKEN is being offered to customers in China or elsewhere, either by handset manufacturers or telcos. Advertising of CHAKEN is limited and only comes from a few smaller businesses rather than the titans of industry that were named as contributors to the standard. Personal correspondence with a representative of Huawei confirmed that there had been no active push to make CHAKEN available in practice.

It is not unusual for technologists and academics to develop standards that gain no traction in real life. This paper also covers several other examples. However, the source of this standard and its official abbreviation in English – a deliberate play on the concept of a Chinese SHAKEN – begs questions about the motives behind it. Might implementation of CHAKEN be ramped up as a rival to SHAKEN if China's government perceived there was a serious risk of SHAKEN being adopted in the Southeast Asian countries that it most needs to work with to reduce scams? Does China (correctly) perceive its interests to be threatened if the USA succeeds in imposing a centralised transnational governance structure for international calls authenticated and traceable through SHAKEN?

The US model of allowing US-domiciled nonprofit corporations to oversee much of the governance of the internet conflicts with China's desire to transfer oversight to the United Nations. Research into CHAKEN may ultimately be motivated by China needing alternative diplomatic options if a US-dominated SHAKEN gains wider usage across international telecoms markets than it has so far.

Proven effectiveness so far	1	There is no evidence of this ambitious technology being demonstrated in practice, despite the involvement of some of the world's largest and most prominent technology companies
Range of communication channels covered by the method	3	The initial scope would be voice calls over SIP networks but an architecture which ties authentication to the handset would be more readily extensible to other services delivered through the handset than a method which ties authentication to the telephony network provider
Range of uses covered by the method	7	CHAKEN would deliver all the capabilities promised by the STIR/SHAKEN family of protocols while making them more sophisticated and making them all available to every consumer, with none of the anti-imposter features being limited to enterprise users
Market readiness	1	The standard was published and formally approved in 2024 but there has been scant evidence of it being readied for the market since
Anticipated cost of implementation	0	The lack of any market penetration suggests considerable additional investment would be needed just to bring the technology to market
Style of traceback	Direct, if each handset that receives an authenticated call maintains its own log then this could be used by law enforcement to identify the A-party for those calls	
National security	As CHAKEN is likely positioned to stymie US security interests, its international adoption would give rise to parallel national security risks for the EU	
Score	12	

AB HANDSHAKE

AB Handshake is both the name of a proprietary voice call and SMS authentication and tracing technology and the business that supplies it. The technology is the subject of several patents owned by the company[1]. The company is nominally headquartered in the USA but is an offshoot of LANCK Telecom, an international wholesale carrier founded in Russia in the late 1990's. LANCK later changed its domicile to the USA as well.

The AB Handshake authentication method is essentially a peer-to-peer out-of-band exchange of data using servers connected to the internet. Each telco would set up their own server, and the servers communicate with the relevant peer at the beginning and end of a call, thus providing two-way verification that the A-party reached the correct B-party and permitting the B-party to confirm the identity of the A-party.

Lavish claims have been made about the number of businesses using the technology to authenticate calls but there are no known customers on public record. Given the relationship between AB Handshake and LANCK Telecom, it is likely that LANCK is using the technology and that claims about the extent to which this method has been adopted across the telecoms industry reflects the international clientele for LANCK's wholesale services rather than communications providers that have chosen to implement their own authentication servers.

Given the provenance of AB Handshake, and the lack of information about how data is secured, any interest from the EU would be predicated on receiving assurances about the privacy safeguards that have been implemented. A system that collects and retains data about who is calling whom and who is sending text messages to whom represents a potential source of signals intelligence for surveillance bodies.

Proven effectiveness so far	3	AB Handshake began filing patents in 2020, soon after its incorporation, and it has been marketing its authentication technology through reputable industry associations since but the effectiveness of the technology is difficult to evaluate due to the absence of any independent information about who is using it and the results they have obtained
Range of communication channels covered by the method	5	The patents cover both dialled voice calls and SMS, but the architecture lends it to future extensions to other communications services
Range of uses covered by the method	5	The two-way validation checks would identify a broader range of business-on-business frauds than most other methods reviewed, in addition to providing anti-scam authentication and traceback to protect consumers
Market readiness	3	As stated above, forming a conclusion is difficult due to limited evidence
Anticipated cost of implementation	10	The method is simple and marketing emphasises that the system was designed to run on low-cost and readily available commodity hardware
Style of traceback	Direct	
National security	Assurances would be needed over how the privacy of data will be maintained	
Score	26	

[175] <https://patents.google.com/patent/US10951775B1/en>

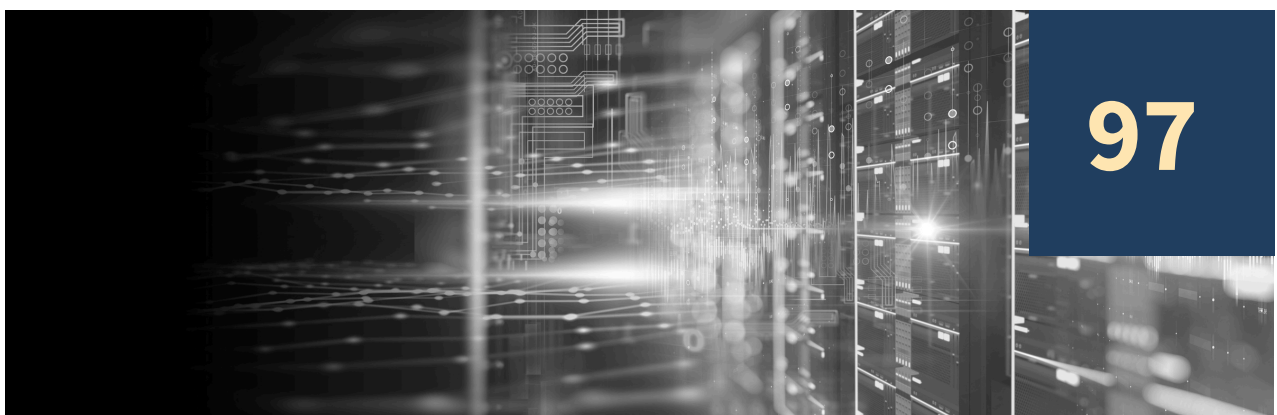
Open Verified Communication is a technology being cooperatively developed by multiple businesses under the auspices of the GSMA [176]. Given the overlap in membership, it is highly likely the technology will be endorsed by One Consortium in future. OVC takes some of the concepts instantiated in STIR/SHAKEN as a starting point while addressing some of the weaknesses of STIR/SHAKEN that have inhibited its adoption outside of the USA. The functional advantages of OVC over STIR/SHAKEN are as follows:

- OVC can be applied to text messaging as well as dialled voice calls
- OVC authentication data can agnostically be carried in-band or out-of-band
- OVC establishes the A-party's right to use the originating address through a technological pathway that allows that right to be tied to the forms of digital identity resulting from eIDAS instead of requiring that the customer's identity can only be affirmed by their communications network provider
- OVC does not assume there will be a single governance authority but permits multiple governance regimes to apply in parallel to the same communication services

This work is all very promising. But if every promising new technology came to fruition, then the challenge of how to trace communications and prevent spoofing would have been overcome years ago. It is not hard to imagine ways that the advantages in the design of OVC could be corrupted as more businesses and more nation-states take an active interest in the technology. For example, we have already seen how little progress has been made with out of band SHAKEN because of factors unrelated to the goals of consumer protection or law enforcement, and something similar could happen with the out of band varieties of OVC. OVC, like CHAKEN, creates the potential for authentication to flow from handset to handset without necessarily being controlled by telcos, which could potentially lead to resistance because of the diminishment of the business opportunity for telcos to generate revenues from the authentication of their users.

It is too early to confidently predict the final shape of OVC, but the work so far at least demonstrates it is possible to design authentication systems that work like SHAKEN without all the weaknesses inherent to the US implementation of STIR/SHAKEN.

[176] https://www.gsma.com/solutions-and-impact/technologies/mobile-identity/gsma_resources/mwc26-barcelona-mobile-identity-summit/



Proven effectiveness so far	4	Multiple businesses have worked together to demonstrate the technology works on a small scale for dialled voice calls; the next trial will involve text messaging and there is a need to ramp up volumes to prove it works at a large scale
Range of communication channels covered by the method	5	The two-way validation checks would identify a broader range of business-on-business frauds than most other methods reviewed, in addition to providing anti-scam authentication and traceback to protect consumers
Range of uses covered by the method	5	The method is simple and marketing emphasises that the system was designed to run on low-cost and readily available commodity hardware
Market readiness	3	As stated above, forming a conclusion is difficult due to limited evidence
Anticipated cost of implementation	10	The method is simple and marketing emphasises that the system was designed to run on low-cost and readily available commodity hardware
Style of traceback	Direct	
National security	Assurances would be needed over how the privacy of data will be maintained	
Score	27	

CIV

Caller ID Verification (CIV) is the name given to a call authentication method devised by British academics and currently documented as draft IETF standards [177]. The research into CIV is led by Professor Feng Hao of the University of Warwick's Department of Computer Science and was supported by a GBP 900,000 (EUR 1.05mn) grant from the UK's Engineering and Physical Sciences Research Council. When applying for this funding, the academics explicitly positioned CIV as a necessary alternative to STIR/SHAKEN that would address two of STIR/SHAKEN's most severe weaknesses:

- STIR/SHAKEN incurs all the costs associated with a Public Key Infrastructure (PKI) while begging the question of who will exercise control over the certificate authorities that centralise power within an international system; and
- STIR/SHAKEN's dependence on SIP.

Their idea was to greatly simplify the process of verifying the origin of an incoming call through a challenge-response cycle. When the B-party first receives an inbound call, it will automatically attempt to contact the number presented as the CLI on the incoming call before the recipient's phone begins ringing. If the CLI is genuine, then the A-party would then provide confirmation. If the CLI had been spoofed, then the request for confirmation would fail.

[177] <https://www.ietf.org/archive/id/draft-hao-civ-03.html>



Researchers are exploring refinements of their method that would minimise the time spent on the challenge-response cycle. For example, one recent focus has been on integrating CIV with Asterisk, free software distributed under a GNU GPL license that is widely used to run phone exchanges on commodity hardware.

The work is promising, but its effectiveness in practice will only be determined by executing the technique at scale under the kinds of loads that occur in real life. The academics responsible for CIV are currently seeking partners in the private sector to help them develop their method. To aid their search for partners, they have approached NICC Standards Limited, a UK association of British telcos that reaches agreement on how their networks interoperate and which is tasked with providing advice on traceback and authentication to the UK government and telecoms regulator. However, their interaction with NICC is only at an early stage. Without assistance from the private sector, the research into CIV will struggle to progress to the phase where it becomes a commercially viable proposition.

Proven effectiveness so far	3	The method has been shown to work at a small scale, and further work is needed to test it under realistic loads
Range of communication channels covered by the method	2	CIV was developed in response to STIR/SHAKEN so is designed to prevent CLI spoofing for dialled voice calls but the principles could later be applied to other channels so long as B-parties are presented with a return address for incoming communications
Range of uses covered by the method	2	The purpose is to identify spoofing but the data stored in a call log could potentially be used for traceback if the log records whether a call was successfully authenticated or not
Market readiness	2	Investment will be needed to test the method at scale and then make it widely available
Anticipated cost of implementation	10	The innate simplicity of the method keeps the cost low
Style of traceback	Direct, if call logs record whether an inbound call was authenticated	
National security	No concerns	
Score	19	



CODEB SOVEREIGN SESSION BORDER CONTROLLER (SBC)

CodeB is a brand of Aloaha Limited, a software business based in Malta. They are suppliers of IP-based communication systems and digital identity solutions. Around 2022, CodeB began marketing the ability to transfer call authentication data out-of-band. The ability to “sign outbound caller-ID” is now presented as a selling point for their Sovereign Session Border Controller, a product that manages the flow of SIP data at the boundary of a network. CodeB has been listed among the tools inventory of One Consortium but does not appear to have been meaningfully reviewed by that association, probably because the business is not a member. The call authentication functionality now offered by CodeB is not prominently advertised on their website, suggesting it has not been a significant driver of sales for them in recent years. For the purposes of this report, no further research has been conducted, and no evaluation is offered, but the fact that CodeB has previously sought to market their call authentication capabilities has been included for completeness.

Score

Not enough information to give a fair evaluation

ITU-T Q.3063

Q.3063 is an ITU standard that was approved in September 2022 that defines signalling requirements and procedures for calling line identification authentication in telecommunication networks using SS7 signalling, the signalling protocol for TDM networks that predates SIP [178]. The core purpose of this standard is to prevent the spoofing of CLIs. China Telecom is listed as a supporting ITU member for Q.3063. Subsequent amendments of other ITU standards were adopted in order to make them consistent with the implementation of Q.3063. As such, this ITU standard sounds much like the kind of material that should be included in this review. However, we can find no evidence of anyone implementing the standard in practice.

Our best estimation is that Q.3063 was delivered too late to have any practical consequences for telcos in the real world. The ITU’s work in this domain has not gained much prominence outside of the ITU. While the transition to SIP may not progress as rapidly as would suit some advocates for SIP-based authentication of calls, the replacement of SS7 networks with SIP networks means there will only be a steady decline in the motivation to invest in implementing a call authentication method based on SS7. Those countries which are most interested in implementing methods to prevent spoofing will also tend to be the countries that have made substantial progress with the replacement of their SS7 networks.

Meanwhile, research into low-cost out-of-band methods for call authentication that can be applied universally across both SS7 and SIP networks has been sufficiently promising to beg the question of why any business would choose to put Q.3063 into practice. For example, a CP familiar with the more prominent work that has gone into out of band SHAKEN would likely reason that applying out of band SHAKEN to its SS7 networks would incur significantly less risk of premature irrelevance.

Score

Not relevant to deciding the future of call authentication in the EU

[178] https://www.itu.int/ITU-T/workprog/wp_search.aspx?isn_status=-1,2,5&q=2&sg=11&sp=17



HEKSAGON CALL VERIFICATION SERVICES

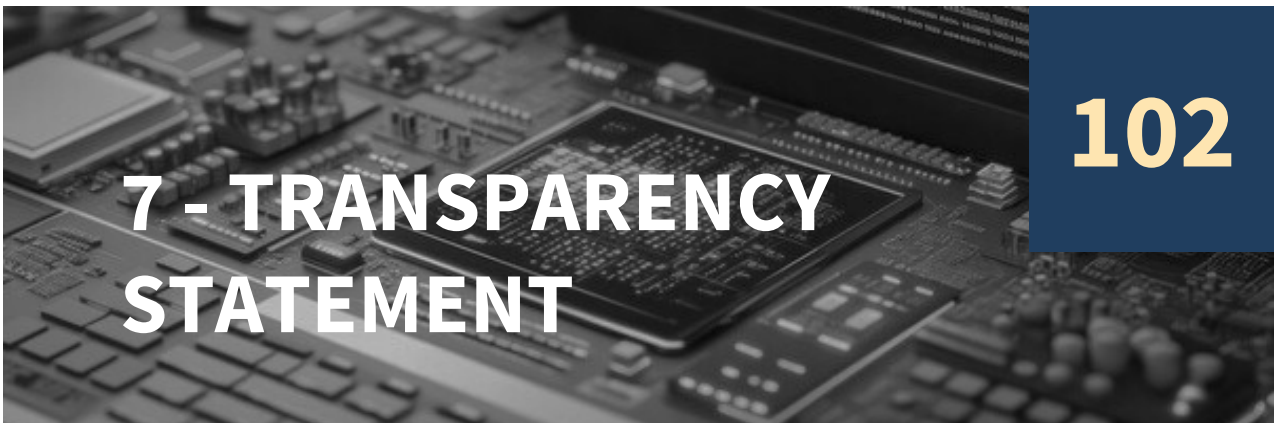
Heksagon is a telecoms software business headquartered in Serbia. Their suite includes anti-fraud products. The business is a member of the GSMA and One Consortium and it actively engages with the work done by those associations of relevance to this report. Their name is listed among the tools inventory of One Consortium, but we could not find evidence of a relevant product being meaningfully reviewed by that association. Heksagon submitted a response to our open survey, as repeated in full within the survey annex below. This response describes many desirable qualities of systems that would need to support the traceback and authentication of communications. However, it appears that this is being described in the context of Heksagon being a supplier of firewalls to communications providers, not in the context of a unique method to exchange data that might be acted upon by firewalls.

The other methods covered by this review essentially relate to methods to exchange data (STIR/SHAKEN, Oculeus 2FN, OVC, etc.) or procedures to act upon the data that is available (ECC Recommendation (23)03, SMS Sender ID registries, etc.). There are other suppliers of firewalls, and a comprehensive review of the strengths and weaknesses of different firewalls would be well beyond the scope of this review. Methods to exchange data would need to ultimately integrate with firewalls if the firewall is being used to block a spoofed or unauthenticated communication. While it is pleasing that Heksagon has anticipated the need to integrate with those methods of exchanging data, it is also reasonable to suppose that other suppliers of firewalls will adapt their products if an authentication or tracing method gains sufficient market penetration to make the changes worthwhile.

For these reasons, Heksagon and its submission to the survey is included in this review for completeness, but no evaluation is offered.

Score	Outside of the scope of this review
-------	-------------------------------------





7 - TRANSPARENCY STATEMENT

102

This statement is provided for transparency purposes, **highlighting possible conflicts of interest**. 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, comparative evaluations, scores, rankings, observations and recommendations presented herein 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. The views, assessments, conclusions and recommendations presented in this report do not reflect ENACT's opinions and should not be interpreted as an endorsement, approval, or recommendation of any particular technology, provider, product, service, methodology or 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.

8 - RECOMMENDATIONS

Comprehensive adoption of ECC Recommendation (23)03

Complete the implementation of blocks of inbound international calls that spoof domestic calls in all EU countries, including the implementation of roaming status checks so spoofing of CLIs associated with mobile phone numbers can also be identified. Use the development of data exchanges for roaming status as a practical starting point for developing transfers of anti-scam intelligence between telcos in different EU countries.

Federated Sender ID Registries

Implement SMS Sender ID registries in all EU countries. Agree common principles across the EU so the registration process can be federated. A federated process would both increase the protection across the EU while allowing an entity to register the same Sender ID in multiple countries at the same time.

Determine Traceback Volumes Realistically Required in Practice

It may be tempting to ask for more sophisticated technologies that can handle many more traceback requests, but the design of new systems should reflect the demands that will be placed upon them. A half-billion Euro system would represent a poor investment for the EU if it will only be used to facilitate a few thousand traces per year, and if LEAs lack the resources to act upon the intelligence in those traces.

The starting point for a design should involve a realistic appraisal of how many traces LEAs would be able to act upon during a year, given the resources available to LEAs.

It is likely that a low-volume traceback process could be made more efficient by simply standardising the way traceback queries are communicated to CPs and the deadlines for them to respond.

An appraisal of the requirements should also cover the strategic goals to be satisfied. Is the primary aim to tackle scams originating in scam compounds in Southeast Asia? Or scams that originate within the EU? Or other kinds of crime? A better understanding of who would need to support a traceback system will help with ensuring the goals are realistic.

It would help with ensuring alignment with the negotiation that most occur with other countries about how a traceback system would work in practice. Such negotiation would cover whether local systems are backed by sufficiently robust KYC controls and whether there is a realistic prospect of extradition and punishment of the A-parties that would be identified by traces.

Identify Bilateral Partners Outside of the EU

It follows from the previous recommendation that tracing systems should be tailored to the circumstances faced by those countries outside of the EU that would be willing to enter into bilateral agreements for the exchange of tracing data.

In particular, work towards out of band methods that can be implemented at the origin and destination countries would accelerate the delivery of results for LEAs by eliminating effort on intermediate countries. Agreeing low-cost methods will make them more attractive to bilateral partners. Implementing a bilateral arrangement for a system between a particular country and the whole of the EU would spare each EU country reaching its own agreement. It would also clarify if there are particular legal constraints that affect the exchange of data involving some particular EU countries.

A Register of CPs

The EU should create a consolidated register of businesses that would need to support international traceback in the style of the US Robocall Mitigation Database. The most essential data in the database would be the contact details of people who are responsible for responding to traceback queries.

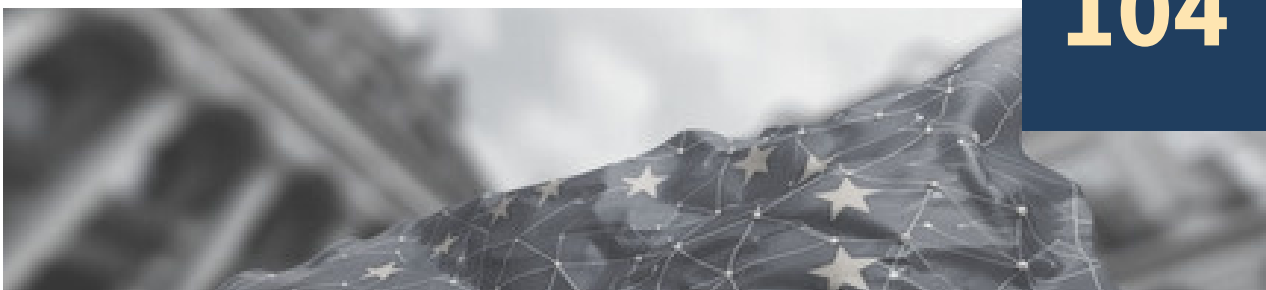
Creating this register for the whole EU would reduce the duplication of effort that would be involved in each nation collecting the same data. It will also reduce the burden on CPs that would need to provide information and assist with traceback queries.

Penalties for Being Unhelpful

The most obvious problem with asking CPs to help with traces is that they may not help with traces, especially if the CP is based in another jurisdiction. For a realistic chance of success, the EU needs to consistently legislate to create obligations for foreign CPs to assist with traces and penalties if they refuse. These obligations should at minimum include providing timely updates of information for the Register of CPs and the contacts listed therein, and a maximum amount of time that CPs have to acknowledge and respond to traceback queries.

Federated DNO

National Do Not Originate lists are an effective way to prevent impersonation of phone numbers used for incoming calls by government entities and big brand businesses. Given the free movement of EU citizens across borders, the existing DNO lists should be federated, ideally alongside the federation of the SMS Sender ID registrations. Providing a comprehensive EU-wide integrated service for logging phone numbers and Sender IDs leaves fewer loopholes for scammers to exploit and will make it easier for businesses to register their interests across the whole of the EU.



ANNEX A: SPOOFING AND TRACEBACK SURVEY QUESTIONNAIRE

This annex reproduces the questionnaire. The responses received can be found in a separate online Annex where respondent wording is reproduced as submitted.

A1: 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.

- Email address
- Telephone number, including country code





[@enact-network](https://www.linkedin.com/company/enact-network)



enact-eu.net



Scan the QR code to visit ENACT online
and read this report in digital format.



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 Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.