ONE CONSORTIUM

International Traceback High Level Outline

Release 1.0 – May 2026

Traceback – An overview of the landscape

This document is aimed to be a guide for implementing and operating traceback solutions across the telecoms industry, including but not limited to, network operators, regulators, enforcement organisations, and consumer representative groups. It describes how existing traceback solutions work and highlights some of the benefits of operating national traceback solutions. It also looks forward to how traceback might be made more effective in an international context as well as identifying some of the challenges with cross-jurisdictional implementations. It has been put together by the One Consortium Traceback Working Group in collaboration with GIRAF.

This document is the first step of the work of the Traceback Working Group that will continue to research this space in more detail and propose a framework and/or best practices for traceback to the industry. The focus of our efforts includes looking into: possible roadblocks and problem use cases, the legal basis for traceback in different jurisdictions, operational considerations, and technical implementation options. This will be done through continued engagement with GIRAF.

Date	Version
18 Feb 2026	0.1
5 May 2026	1.0
This document is intended to be a living document. It will be reviewed periodically and updated as operational experience, regulatory developments, and industry practice evolve.	

Overview

Traceback is a process to identify the true source of a telephone call. Where authoritative originating information is available, for example, call authentication information, calls may be immediately traced back all or part of the way to their source based on such information instead of tracing hop-by-hop through every intermediate carrier. Where such information is not available—as well as to provide transparency and accountability about illegal calls throughout the call path—traceback can be initiated to determine the path a telephone call took, potentially through multiple communications networks, and identify the true source of the call. Beginning with a terminating voice service provider—whose customer has been harmed—a call can be systematically traced from one voice service provider to the preceding voice service provider network until a non-cooperative voice service provider and/or the originating voice service provider or originating customer is identified. Even when this hop-by-hop approach does not yield the caller's identity, the process and data collected provide valuable insights for policing networks. As described in this paper, different tools may be used in combination to identify the true source of the call depending on the need.

When a traceback is confined to a single jurisdiction, the relevant laws, rules, and commercial frameworks should be uniform and understood by all participants. When tracebacks extend beyond a single jurisdiction, differences in legal frameworks, privacy protections, and operational practices can create friction. To make traceback workable, ideally there is at least a baseline set of principles, guidelines, or legal provisions that—even if not identical—enable consistent participation and cooperation across jurisdictions.

With this report, One Consortium provides an overview of traceback, defines key principles for its deployment, and identifies challenges that arise in tracing both domestic and international calls. With that goal, One Consortium aims to assist regulators with understanding traceback and providing advice on how to best implement traceback solutions, including how to make these operate effectively in a global context.

About traceback

Purpose of a Traceback (Why do we do it?)

Voice calls are a key fraud pathway, particularly given the persistence of number spoofing and the global reach of scam operations. A proven mechanism to identify those responsible for call-based fraud—whether domestic or originating overseas—is traceback, also known as call tracing. When properly deployed and managed, traceback can pinpoint the source of a call within hours or days, in contrast to the extended timelines law enforcement faces when obtaining equivalent data through formal investigative procedures or mutual legal assistance mechanisms. Beyond law enforcement, traceback also enables carriers to better police their own networks and allows private enterprises to use verified data to protect consumers, brands, and communications from scams and other abuses.

Types of Traceback Processes

In existing solutions, a telecom provider (usually the terminating provider) checks its records to see which provider sent a particular call to its network. This can be a complex process when providers use multiple systems and networks to receive calls. As an example, where there are three "hops," once the inquiring

provider (“hop 1”) identifies a call source, it asks the provider that sent the call (“hop 2”) to identify where the call came from (“hop 3”). The inquiring provider then, in turn, asks every provider in the call chain until the call source is located. Examples of existing traceback processes are discussed in detail in the attached 'Traceback process overviews', but include:

Provider-to-Provider

These tracebacks require communication among participating carriers and are handled through agreed upon means (secure messaging for example) to directly share information with no centralised or active management.

Centralised Coordination

In other scenarios, there is a central coordinator such as a regulator or a neutral third party. These processes may be largely manual, using specified forms managed by the central coordinator or be platform based, automating much of the work of the traceback, such as routing the request to the relevant telecom providers (the “hops”) and logging the progress of the trace. The traceback platform approach allows multiple providers across jurisdictions to collaborate while keeping the data confidential to the appropriate parties and enabling efficient administrator-driven management, communication, and education, as well as efficient provider, enforcement, and data partner utilization of the process while keeping underlying data subject to appropriate controls informed by domestic regulation, laws, and other considerations.

Trace Forward

These Tracebacks are forward-looking. If criminals are using geographic, national, or toll-free call back phone numbers, an investigating provider also has the option of tracing the use of the call back number itself. This is called “trace forward.” Rather than enquire about the origin of an incoming call, the investigator can enquire about the subscriber of the call back number. This assumes that the scammer has ownership of the number, which can be easily determined by verifying scam victims called the number and reached a scammer or by having an investigator call a scam number themself. The advantage of trace forward is that it typically involves fewer enquiries than traceback, and all customers who placed calls to a scam DID can be identified as potential victims.

Information Needed for a Traceback

Required

Data typically required to initiate a traceback includes

- originating telephone number;
- called telephone number;
- date and time of call;
- reason for traceback*

* It would be useful if the reason for a traceback was selected from a standard list of reasons that is regularly maintained. This will be useful for ongoing reporting and trend analysis.

Optional

Other data that can be useful for an investigative and evidentiary standpoint includes:

- originating IP address or Originating and Destination Point Codes;
- called IP address;
- Session Initiation Protocol (SIP) header anomalies;
- evidence of Caller ID, Automatic Number Identification (ANI), telephone number spoofing;
- volume of calls, including call detail record (CDR) file information;
- Information about Voice Service Providers in the call path.

Information Provided from a Traceback – Uses and Applications

Traceback results can provide valuable insight into the origin and even the behaviour of fraudulent or unwanted calls. Used responsibly, traceback data can therefore serve not only enforcement goals but also broader prevention, education, and industry hygiene functions—helping networks collectively reduce exposure to fraud, scams and spoofed traffic.

Direct Use of Data

Data can identify recurring routes, origination points, or providers associated with high volumes of suspicious traffic. Over time, data can support more strategic interventions and improve the targeting of mitigation measures.

Identification of Persistent Bad Actors

Repeated traceback results that point to the same originating provider or customer can help identify persistent bad actors or networks that enable unlawful traffic. This intelligence supports network remediation, contractual enforcement, and regulatory oversight.

Evidence for Law Enforcement

Traceback information provides structured data in a standardised format that can assist law enforcement investigations by significantly shortening investigative timelines with consistent records of a call path from a single source.

Data Sharing and Reputation Insights

When shared under appropriate privacy and legal safeguards, aggregated traceback outcomes can inform industry reputation systems, risk scoring, and international cooperation. They also enable providers to identify emerging fraud trends and strengthen their own network protections.

Traceback Criteria

To safeguard individuals' rights to data protection and ensure privacy of communications, it is critical that high standards apply when a requesting authority initiates a traceback. Tracebacks should only be initiated for calls that are highly likely to be illegal within the jurisdiction of the requesting Authority. For example:

> *"Calls made (often without the recipient's consent) that violate local laws or regulations or when a relevant Authority is investigating a crime and where establishing information about the calling parties would assist the investigation"*

Traceback requests should only be initiated per local regulations, e.g., law enforcement or judicial process, and in full compliance with all relevant domestic processes. Traceback requests should be initiated in accordance with local regulations when there is reasonable potential for harm, e.g., call volume, potential monetary harm, or when undertaken in conjunction with a wider criminal or civil investigation and where the relevant authorities are entrusted investigatory powers that include traceback.

To protect the rights and interests of providers and others, there must be a manageable definition of traceback candidates. For example, in the United States, by law, tracebacks are done to identify sources of illegal, fraudulent, or abusive traffic. Tracebacks are initiated only if

- A credible and verifiable source* is providing information regarding the traceback candidate;
- The nature of the traffic associated with the traceback candidate is deemed after due diligence to be fraudulent, abusive, or unlawful;
- Initiation of the traceback warrants utilisation of the systems resources.

** 'A credible and verifiable source' will need to be defined in greater detail as this may differ by jurisdiction*

Traceback solution

Suggested Operating Principles

Below are some of the principles that would be beneficial for this framework to adopt to ensure effectiveness and adoption.

Principle	Explanation	Benefit
Neutral	Any cross jurisdictional governance should be neutral	• This will help to encourage maximum participation and ensure trust in the solution
Interoperable Platforms	Traceback platforms should be interoperable. This can involve agreeing standardised APIs (for example under the framework of CAMARA)	• This will allow each jurisdiction to retain governance of their own part of the traceback process and allow interworking with existing in-place solutions maximising the fight against global fraud
Industry led	The initiative should be industry led with wide participation across the industry	• The industry is best equipped to understand the challenges, • In some cases, Industry can take measures to block or mitigate traffic based on consistent bad actors • Encouraging collaboration both nationally and globally will yield the best results
Collaboration with regulators	Deployments of interoperable solutions should involve the applicable jurisdictional regulator and include collaboration amongst National Regulatory Authorities (NRAs)	• NRAs can encourage operators to participate • Will ensure domestic solutions work smoothly and meet requirements for interoperating • Assistance with negotiating in-country challenges and privacy laws
Partnership with law enforcement	Deployments should include close collaboration with law enforcement	• Ensures the solution is best adapted to assisting law enforcement and provides timely and useful information • Establishes a good effective process and encourages participation from law enforcement • Assists with understanding local characteristics of specific requests • Law enforcement already has separate channels and requirements that may not be compatible with an international system of traceback (e.g., investigation secrecy)
Timely	Deployments should aim for rapid results and be driven by Service Level Agreements (SLAs)	• Ensures the system is useful at preventing problematic traffic • Aligned SLAs encourage timeliness without making adoption a burden

		• Different jurisdictions will have different internal requirements and SLAs that could make this challenging in an international context
Flexible	Solutions need to be flexible, adaptable, and extensible	• Ensures that traceback can remain relevant in a fast-changing environment • Ensures traceback can adapt to new industry threats • Ensures traceback can work alongside new industry initiatives that may be adopted in the future while providing value now
Feedback and review	Solution needs to have a mechanism for regular feedback and review by participants	• Allows processes to be improved • Allows highlighting of slow responses or non-cooperation • Allows sharing of statistical data and trends
Clarity	• Provide methods to specifically identify operators • Provide single points of contacts within operators	• Allows clear attribution to operators • Speeds up communication • Allows for statistical analysis • Allows for analysis of operating the solution and allocation of cost per traceback corridor
Integrity	Ensures traceback results and process cannot be tampered with by bad actors	• Ensures trust in the system

Encouraging participation

Encouraging broad participation in traceback requires a mix of regulatory direction and clarity, industry awareness and incentives, and operational practicality. The following elements can help motivate cooperation across jurisdictions and provider types:

- **Regulatory encouragement:** Regulators can play an important role by promoting traceback participation as a standard expectation of good network stewardship and compliance. Public endorsement or inclusion in regulatory frameworks increases confidence and accountability.
- **Potential declaration of cooperation:** A formal declaration can signal government support and set clear expectations for participation, including commitments to privacy, transparency, and due process.
- **Law enforcement interest and partnership:** Law enforcement agencies can encourage cooperation by demonstrating the real-world value of traceback participation and by treating all participants as trusted partners. Public acknowledgment reinforces traceback as a credible, outcome-driven process.
- **Market pressure:** Industry participants may increasingly avoid partnerships with non-cooperating carriers. Over time, refusal to participate in traceback may carry reputational or commercial consequences, reinforcing cooperation as a business norm.

- **Education and awareness:** Demonstrating the operational and reputational benefits of traceback—such as keeping fraudulent or abusive traffic off networks—encourages voluntary participation and helps providers understand how cooperation protects customers and brands alike.
- **Ease of implementation:** Traceback processes and tools should be simple to adopt, with clear procedures and minimal administrative burden. Automation and standardization can make participation routine rather than exceptional.
- **Low cost:** Participation should not require significant new resources making engagement practical for providers of all sizes.
- **Safe harbour for cooperation:** Providers that participate in good faith should be protected from enforcement actions solely because they were in a call path that included unlawful traffic. Clear safe-harbour language reinforces confidence to cooperate without fear of unintended liability.
- **Legal clarity:** Clear regulatory guidance on data-sharing exceptions, privacy obligations, and existing safe harbours enables providers to respond to traceback requests efficiently and lawfully.
- **Reciprocity:** Participation should come with the reciprocal benefit of being able to initiate or request tracebacks. This shared responsibility fosters mutual accountability and strengthens the overall system.
- **Private sector engagement:** Enterprises and brands (financial institutions for example), can use traceback data to identify and disrupt scam campaigns, demonstrating the broader societal and commercial benefits of participation.

Potential Challenges

There are many potential challenges to deploying traceback solutions, particularly given the need to ensure global collaboration. The hop-by-hop nature of existing traceback solutions means that broad participation is essential to ensure effectiveness of traceback. Below are some of the potential challenges to adoption and success along with some mitigations that can help ensure positive outcomes.

Potential challenge	Details	Potential mitigations
Privacy laws	Different jurisdictions have different privacy laws that will in some cases conflict with the requirements of traceback and the sharing of data	• Limit the data that can be communicated in certain case or by obfuscating the data where required • The solutions should only exchange data that is necessary for traceback and not exchange extraneous data • Ensure differential data disclosure where required

		• Regulators could clarify the interaction between traceback requests and privacy laws • Education and guidance on existing safe harbours and carve outs in privacy regulation
Getting sufficient operator participation	Encouraging operators to get involved will be challenging, and the system works best with broad adoption.	• Make the framework solutions as easy, cheap, and simple to adopt and operate as possible • Regulatory encouragement • Industry driven encouragement of cooperation • Ensure the system has an impact on the problem and that its success is well publicized • Ensure there are consequences for non-participation either industry or regulator led
Countries never participate	There will be some countries that are less willing or unwilling to participate	• Ensuring traceback solutions can interwork • Ensuring the system has an impact on the problem and that its success is well publicised
Cross border law enforcement may not be able to act	Even if traceback solutions are effective, ensuring action in taking on bad actors may be more challenging that may reduce the framework's success	• Provide as much support for law enforcement and work with cross-border agencies to maximise effectiveness • Encourage industry led prevention measures (traffic identification and blocking) driven by close collaboration

The role of the regulator

Regulators play a central role in establishing confidence, consistency, and accountability in traceback operations. Their leadership helps ensure that traceback processes operate lawfully, efficiently, and in alignment with national policy objectives while fostering cooperation among providers, enforcement agencies, and private entities. At a minimum, regulators should ensure:

- Oversight of traceback operations: While traceback should be industry led, regulators should maintain appropriate oversight of how traceback is conducted within their jurisdictions to ensure integrity, compliance with local law, and alignment with national enforcement and consumer protection priorities.
- Regulator as a customer: The regulator can act as the primary "customer" or beneficiary of traceback outcomes, using the findings to inform policy, guide enforcement priorities, and assess systemic risks.

- **Encourage or mandate participation:** Regulators can encourage—or where appropriate, require—communications providers to cooperate fully in traceback, supported by clear mechanisms for secure data sharing and information exchange.
- **Promote safe harbour provisions:** Regulators can help establish or clarify safe harbour protections for providers that participate in good faith, ensuring they are not penalized merely for being in the call path of unlawful traffic.
- **Provide privacy guidance:** Regulators should issue clear guidance on how privacy and data protection laws apply to traceback, including practical advice on lawful data handling and disclosure.
- **Highlight existing privacy carve-outs:** Where existing legal frameworks already allow data sharing to prevent or investigate fraud, regulators should highlight those provisions to reassure participants and expedite cooperation.
- **Clarify provider responsibilities:** Regulators can provide straightforward guidance to communications providers about their obligations and expectations under the traceback process, reducing uncertainty and administrative burden.
- **Encourage broader use of traceback data:** Regulators should promote non-law-enforcement uses of traceback results—such as trend analysis, prevention strategies, and consumer education—to maximise the process's value and deterrent effect.

Governance

This section of the paper addresses what should be considered when setting up a traceback solution. Traceback processes should be public/private partnership to ensure industry cooperation and protection. As regulators promulgate rules for their traceback process, service providers should be consulted to that ensure rules and regulations are technically accurate and feasible. Traceback rules and regulations should mandate carrier cooperation while providing a safe harbour from liability so participating carriers can legally share the requested information without concerns that they will be penalised because bad traffic crossed their networks or for other reasons, such as breaching privacy regulations. In addition, carriers should work together to produce a minimum set of "best practices" to ensure all carriers are following the same guidelines and therefore providing a united front against illegal and unwanted robocalls, allowing regulators to easily identify carriers that are not acting in good faith.

A request to traceback a call that traverses multiple international jurisdictions should be accompanied by protections from regulatory bodies of jurisdictions involved in the call path to ensure safe transfer and protection of both information transferred and the providers involved in the process. Coverage of all carriers in the call path will facilitate the mandate that carriers cooperate in traceback by providing the necessary legal protection, so carriers can share the information requested without concern of liability, such as customers claiming privacy was violated or incurring enforcement action from regulators.

Effective governance of traceback solutions is important to ensure that they can operate effectively. This structure needs to exist in order to enable the sharing of data between carriers and traceback systems,

whether or not all carriers involved in the traceback reside in the same jurisdiction. The Regulators should ensure their process includes safeguards for providers when required to share information with regulators or international carriers, not just nationally. These regulatory processes need to strike the right balance; lightweight regulatory involvement providing just enough regulation to support the process and provide legal safe harbours will be easier to implement. Not having at least some limited data sharing on an international basis could limit the insights that could be gained from information exchanged in a global context.

Operational involvement for cross-jurisdiction collaboration

By encouraging cooperation between domestic traceback solutions and providing a framework around which they can inter-operate, a solution can be created that allows for traceback of calls that cross jurisdictions without requiring any form of central operations.

Actions that could help to support this approach are:

- Creating standard formats for requests and responses
- Defining and publishing standard APIs for communication between systems (perhaps under the framework of the CAMARA project)
- Agreeing processes for interactions between jurisdictions with relation to
    - Privacy
    - Legal basis for a request
    - Passing requests between jurisdictions
    - Applying industry driven sanctions on bad actors

There are areas where a global view may be of use, but these are perhaps outside of operations. For example:

- Providing a global view of statistical trends and data
- Identifying operators on a global basis
- Setting some of the standards listed above

Traceback Process Overviews:

Three known processes currently in use are described below.

Traceback overview - NICC Standards Limited (UK)

In the United Kingdom, an optional, manual traceback process was first published and introduced in 2013. This optional, manual traceback process is described in ND1437. ND1437 was produced by NICC Standards Limited, which develops telecommunications technical interconnect, interoperability, and end-to-end standards, but only when international standards cannot be used or adopted for use in the UK.

In order to trace a suspect call, a consistent approach is needed between authorised requesting organisations (e.g. the UK regulator and other investigators) and the communications service providers (CSPs) whose networks are involved in the call, both in terms of the process and information flow that is used between them. ND1437 describes the information that is required and needs to be available to trace nuisance or unwanted calls between networks and the information that is expected and available in the tracing response. It describes types of call tracing and processes for requesting such call tracing.

ND1437 traceback is a key tool for identifying the true originating CSP behind spoofed or withheld marketing calls made by companies in contravention of the UK Privacy and Electronic Communications Regulations. Authorised investigators have reported a significant increase in spoofed traffic, increasing the reliance on the NICC tracing process.

The operational challenges are around poor CSPs awareness or understanding of this optional NICC trace process, largely due to staff turnover or limited training, or hesitation to disclose information despite proper authorisation, often due to concerns about repercussions from clients (data protection issues). It is also recognised that the process can be complex, requiring escalation to engineers and detailed manual spreadsheet completion. In some cases, this results in delays as requests move upstream, with repeated issues at each CSP. Unfortunately, some CSPs fail to respond or initially deny holding data, later providing it only when pressed. However, typical traceback durations range from a few days to several weeks, although they never exceed 28 days.

Despite the challenges, the process in ND1437 is seen as productive and has supported successful investigations in the UK. It is anticipated that future use of the process will increase due to rising spoofed and overseas traffic.

NICC Standards Limited published a report to Ofcom exploring the challenges and opportunities when implementing a more effective, faster and (perhaps) automated traceback mechanism for scam and fraudulent calls in the UK. The report outlines current practices, both domestic and international, and proposes a set of strategic considerations for a UK-specific solution. The report emphasises the need for a secure, scalable, and collaborative approach involving all stakeholders, including CSPs, regulators, and law enforcement. NICC ND 1527

Traceback Overview: The Industry Traceback Group (US)

In the United States, traceback efforts are coordinated by an industry-led consortium that began as a voluntary industry initiative but now also operates with formal regulatory recognition and oversight. The Industry Traceback Group (ITG) was established in 2015 as an industry-led, non-profit consortium to combat the rise of illegal and spoofed nuisance calls and has since evolved to tracing all types of call abuse. Its success as a voluntary initiative led to formal recognition under Congressional legislation (the 2019 TRACED Act), which resulted in a Federal Communications Commission (FCC) mandate of provider participation and designation of the ITG as the official traceback operator under FCC oversight.

ITG tracebacks are facilitated through a Secure Traceback Portal (STP), which enables rapid, largely automated collaboration across hundreds of participating providers—including non-U.S. carriers. Tracebacks routinely complete within days, if not hours, of initiation, with the median traceback completing in about one day despite an average of 6.9 hops identified per traceback. While the majority of providers still respond to ITG tracebacks manually, the ITG offers API-based participation to reduce operational burden as the effort has scaled. Traceback operates independently of the U.S. STIR/SHAKEN call authentication framework—and preceded deployment of STIR/SHAKEN—though the two can be complementary.

Although based in the United States, the ITG's traceback effort is inherently global: Many ITG tracebacks identify origination outside the country and more than 1,800 CSPs from over 80 countries have participated in tracebacks. To date, the ITG has conducted nearly 30,000 tracebacks, now averaging approximately 1,000 per month. Because the ITG targets representative call samples, these tracebacks reflect billions of illegal calls over time.

The ITG's traceback operation and the STP has streamlined processes that once took weeks into hours or days, dramatically reducing operational burdens for law enforcement, while adding scale to aid detection, disruption, and prevention. In 2024 alone, the ITG initiated over 3,000 tracebacks based on referrals from federal, state, and local law enforcement agencies and responded to over 330 subpoenas and civil investigative demands. Nearly 85 percent of completed ITG tracebacks result in the originating provider warning or firing its offending customer, demonstrating both accountability and speedy disruption.

To support this work, the ITG has developed comprehensive policies addressing key operational, legal, and privacy questions. Per the ITG's sourcing policy, tracebacks are initiated in good faith to stop illegal, abusive, or fraudulent traffic based on self-sourced and acquired data, credible referrals, and alignment with U.S. legal standards regarding call legality. Although the United States does not have a comprehensive federal privacy law (similar to GDPR for example), stringent protections govern the handling of communications data. Traceback activities are conducted in compliance with Section 222 of the Communications Act, which protects certain call record information but allows sharing of call information necessary to prevent fraud and protect network integrity. There are also state privacy laws and enforcement agency protocols. In addition, sensitive provider relationships are protected through controlled access and limited visibility. The ITG's public documentation of these and other policies, which are routinely reviewed and updated as necessary, are available at https://www.tracebacks.org/itg-policies-and-procedures/.

The STP provides differentiated access to support the needs of multiple stakeholders. The ITG administrative team has a comprehensive view across tracebacks, enabling them to assess data sources, initiate and manage tracebacks, identify patterns of unlawful calling, and respond efficiently to legal process through an integrated subpoena response tool. Individual CSPs can access detailed information about tracebacks they are involved in, along with certain aggregate data—such as which upstream providers routinely send them suspect traffic, what mitigation actions were taken, and a dynamic list of CSPs that fail to cooperate. To cooperate with traceback requests, CSPs receive email notification directing them to respond in the STP or otherwise complete the traceback request via an API; the ITG never accesses any CSP system or obtains CSP data directly, and only information necessary to complete the traceback and mitigate the illegal traffic is requested. The ITG is also expanding provider tools, including a due diligence feature designed to help assess prospective network partners based on traceback history. U.S. federal and state law enforcement agencies have limited access to traceback data, such as aggregate data on providers appearing in tracebacks, and must submit a subpoena to obtain further details. All users are subject to terms and conditions governing access and appropriate use of STP data.

Traceback Overview: Australia

Australia's approach to call traceback operates primarily under the Reducing Scam Calls and Scam SMS Industry Code (C661:2022), developed by the Communications Alliance and registered by the Australian Communications and Media Authority (ACMA). The Code establishes a cooperative framework for carriers and carriage service providers (CSPs) to identify, trace, and block scam-related communications.

Under the Code, providers "must have processes in place to trace the origin of alleged Scam Calls" (Section 4.5.1) and are expected to make their *best efforts* to trace "as soon as practicable" (Section 4.4). Traceback requests are typically handled through templates provided by ACMA and with direct provider-to-provider coordination via "an agreed electronic means." ACMA receives copies of cases as well as summary reports on outcomes. C661 also provides for a carrier contact list "[f]or the purposes of meeting the information sharing and notification obligations under the Code." (Section 7).

Data required as set forth in Appendix A of the Code includes: the date and time of the alleged scam calls; the CLI used for the alleged scam calls; the number of alleged scam calls identified in the relevant period; and further evidence if requested by the Originating C/CSP or Transit C/CSP (e.g. customer complaints, call characteristics, CDRs) to support the identified calls as being alleged scam calls rather than legitimate calls.

Sample for Scam Calls information sharing between C/CSPs

Details of Scam Call(s) (Refer to CA G664 Appendix A for a template to provide details)	*[Dates and times, duration, A-Party Number (associated CLI), number of Scam calls in the relevant period, and the relevant CDRs].*
Details of complaints received (if applicable)	*[number of complaints, reported loss, timing of complaints]*
Validation of CLI used for the Scam Call(s)	*[Type and nature of validation checks conducted, e.g., CLI callback, online search yielding evidence of complaints associated with CLI]* *[Outcomes of validation checks, e.g., CLI has been used to perpetrate illegitimate calls, CLI has been used legitimately for telemarketing calls, etc]*

Select from the following:

[Notifying C/CSP] requests that *[Transit C/CSP]* inspect its communications records in relation to Scam Calls detailed above to determine if these are presenting on the Transit C/CSP network.

[Transit C/CSP] should inform [*Notifying C/CSP]* from time to time of the progress of the investigation.

Contact Name: _____

Contact Number: _____

Signed: _____

Date: _____

C661:2022 permits carriers and carriage service providers to share information necessary for tracing and mitigating scam calls, but references the *Telecommunications Act 1997* and the *Privacy Act 1988.*

Information shared under the Code must be limited to what is strictly required for scam prevention and used only for that purpose. The Communications Alliance maintains a list of authorized contacts

7 C/CSP CONTACT LIST

7.1.1 For the purposes of meeting the information sharing and notification obligations under the Code, C/CSPs subject to the Code must register their contact details with CA.

7.1.2 C/CSPs must complete, maintain and keep their contact details up to date on an industry contact list and provide their details to CA within one Business Day for any new addition, or change to contact details.

NOTE: CA will maintain the contact matrix on its website – www.commsalliance.com.au, with updates within 24 hours (one Business Day) of notification of the change. The contact list is password protected.

Example contact list template

Carrier / CSP Name	Phone Contact	Email Contact	1st Level Escalation

https://www.austelco.org.au/wp-content/uploads/2025/06/C661_2022.pdf