One Consortium

The Restore Trust initiative

One Consortium and GIRAF

an update after two years

Industry, regulators & law enforcement
together against scams, globally

On the agenda today

Opening remarks	Philippe Millet, Chair
Keynote	
Europol's initiatives	Martin Kähl, European Cybe Crime Center (EC3), Europol
Latest from One Consortium & GIRAF available on www.oneconsortium.org/publications/	
- Know Your Customer	Keith Buell + Melissa Blassingame
- Spoofing guidelines and GIRAF recommendations	Katia Gonzalez + Thomas Sunesson
- Traceback white paper	Tim French + Linda Vandeloop
- Digital Identity	Steve Buck
- Messaging white paper	Eli Katz + Stacy Graham
- Industry & regulatory surveys + Portal	Tim French + Keith Buell
Closing remarks, call to action	Philippe Millet, Chair

The global Telecoms ecosystem: Industry, Regulators and Law Enforcement together against fraud

Telecoms global contribution to the fight

Prevent, Detect, Stop and Trace Fraud

in a complex and fragmented ecosystem

through cooperation and harmonization

One Consortium

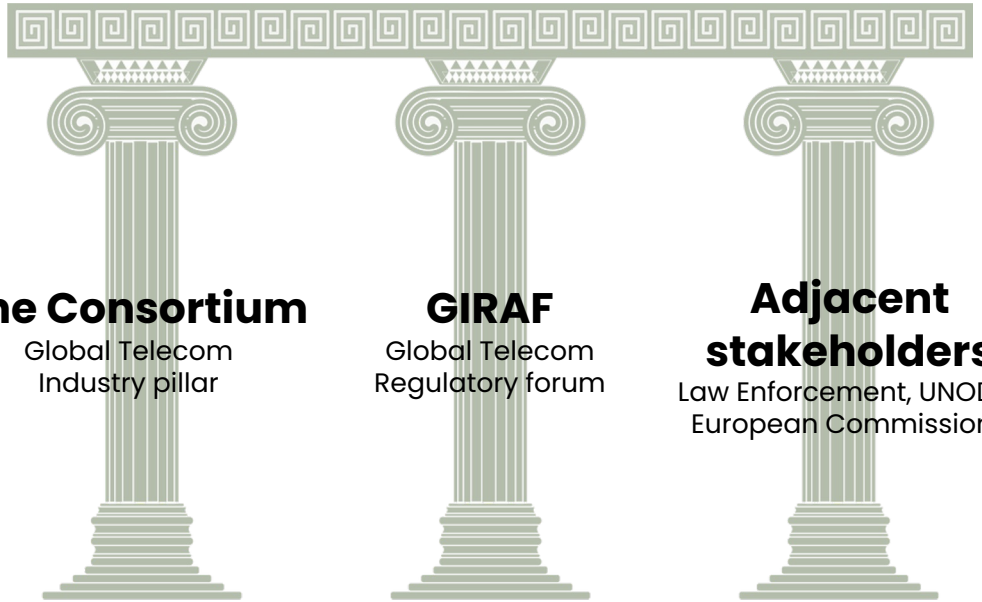
Restoring Trust in telecommunications through multilateral collaboration

64% of scams involve voice calls or SMS (GASA)

only **13% of victims** get all or most of the money back (GASA)

Onlyl **0.05% of all cybercriminals** are prosecuted (WEF)

The Restore Trust initiative



Joint, harmonized, recommendations to build the global Telecoms' response

GIRAF

GIRAF Communiqué

“Carry with Care”

Approved in GIRAF Plenary
November 24, 2025

Supported by One Consortium

Available at
www.oneconsortium/giraf/

The Global Informal Regulatory Antifraud Forum (**GIRAF**), an informal coalition of telecom regulators worldwide, calls on the international service providers (any intermediary player, including international carriers, hyperscalers, aggregators) industry, as one among the relevant stakeholder segments, to take more decisive action against fraudulent traffic.

Fraudulent traffic is so damaging not only to society but also to the industry itself that urgent concrete actions are needed. GIRAF acknowledges positive anti-fraud initiatives by several stakeholders, and at the same time GIRAF encourages the industry to further develop actions to reduce fraud.

Therefore, GIRAF calls for active systematic efforts by international service providers to detect and block fraudulent traffic.

- GIRAF urges stakeholders to take part in international collaborations against fraud such as the **One Consortium** and others to raise awareness, establish best practices and share information.
- GIRAF encourages international service providers to avoid partnerships with service providers that lack robust antifraud policies and practices as per industry best practices and regulatory mandates.
- GIRAF encourages international service providers to provide adequate public transparency on their policies to stop fraud.
- GIRAF underpins that international service providers contracts should have clear descriptions of antifraud obligations such as duties and rights to block, in accordance with relevant regulations.
- GIRAF encourages the international industry to make the necessary contractual alignments ensuring that fraud prevention is financially viable.
- GIRAF encourages international service providers to interact in an effective manner with law enforcement and/or regulators in fraud traceback enquiries, to the extent that information is available.
- GIRAF also encourages regulators and other public authorities to actively engage with international service providers residing in their jurisdiction in order to ensure that appropriate antifraud measures are in place.

GIRAF acknowledges that there could be a need for regulatory guidance on measures to combat fraud eg. on privacy, datasharing and concrete fraud protection measures. Service providers should actively interact with regulatory bodies to seek guidance. In this guidance regulators should take into account in their analyses and interpretations of the regulations, the magnitude of damage caused to individuals and societies by digitally enabled fraud.

One Consortium

Membership
June 2026

Strategic Partners

GASA Global Anti-Scam Alliance

GLF Global Leaders Forum, a techoraco brand

Contributing Members

8x8 · bandwidth · bics proximus · BTS · T · Microsoft · nuso · PCCW Global · consoleconnect · RingCentral · sinch · TATA COMMUNICATIONS · twilio · vodafone · wavecrest · Aegis Mobile · heksagon · netnumber · Numeracle · OCULEUS · PROVENANT · SOMOS · TNS · TransNexus · TransUnion · XConnect A Somos Company

Industry Organizations

atis · CFCA · Cloud Communications Alliance · ctia · COMMS COUNCIL UK · GSC GLOBAL SOLUTIONS COUNCIL · GSMA · i3Forum · INDUSTRY TRACEBACK GROUP · NICC UK Interoperability Standards

Supporting Members

AVISO MESSAGING · COMCAST · colt · iBASIS · identidad Telecom · LUMEN · oni a gigas company · ooredoo · symbio · MTN · 1ROUTE · didXL · Orillion SOLUTIONS · Utel · orange Wholesale

Webinar
One Consortium

Position Paper on Caller ID Spoofing

Anti-Spoofing Initiative

THE GLOBAL THREAT

HUNDREDS OF MILLION

Lost worldwide annually (Spoofing-driven Fraud)

PRIMARY VECTOR

Up to 64% of reported fraud (Phone calls and text)

NETWORK POISONING

Up to 90% of international calls fraudulent (EU MS in 2021)

THE PROBLEM

Spoofing is easy to deploy but hard to trace (LEAs cross-border-investigation)

STRATEGIC PILLARS

TECHNICAL HARMONISATION

Develop traceback mechanisms, standardised signalling checks

REGULATORY CONVERGENCE

Harmonise legal frameworks, mandate service provider validation, define blocking responsibility

COLLABORATIVE ACTION

Real-time info sharing (bypass slow legal processes)
Unified ecosystem (LEAs, ISPs, SPs, NRAs)

EVOLUTION & ACTION

BEST-PRACTICES-MODEL

Direct inter-operator validation, block unverified international using national numbers

KYC & KYT

Strengthen KYC & KYT
Combat SIM-based Scam
Resource Subleasing

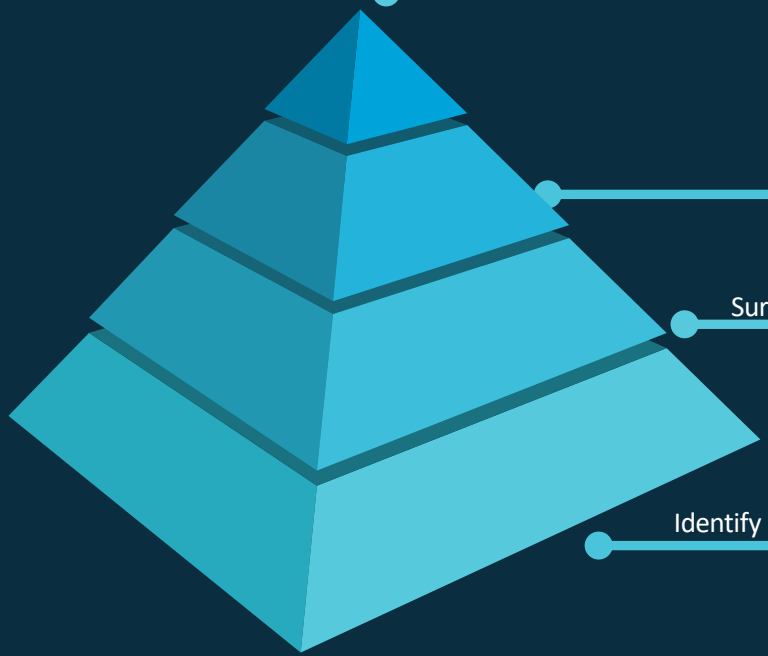
STRATEGIC ALIGNMENT

Integrate defences (PROTECTEU-strategy, DNA)
Safeguard digital trust
Combat organised crime

EMPACT

European
Multidisciplinary
Platform
Against
Criminal
Threats

EMPACT



Pilot Projects on Traceback and Validation

Help initiate and support at least one pilot project to test cross-border traceback mechanisms and call validation models.

D

Framework Development Workshops

Workshops to co-develop a draft framework for harmonised technical standards and converged regulatory policies.

C

Gap Analysis and Best Practice Survey

Survey and categorise the existing technical anti-spoofing tools and initiatives.

B

Stakeholder Mapping and Engagement

Identify and establish formal communication channels with key stakeholders.

A

EMPACT Tracks

Harmonisation of techn. Standards → Industry + ETSI

Cross-Border-Collaboration → LA and Judicial Authorities

Regulatory Convergence → National Regulators + BEREC / GIRAF

Traceback Standardisation

The Strategic Objective:

- Trace calls from the terminating network, back through all intermediate networks, directly to the originating network to empower regulators and law enforcement.

The Friction:

- Traceback processes currently vary heavily by jurisdiction, creating operational bottlenecks.

Caller-ID and Traceback

The Solution: ***Data-Standardisation***

Operational Efficiency	Consistency	Cross-Border Clarity
Standardising the format and structure of data fields speeds up data extraction and handling for network operators.	Ensures regulatory and law enforcement authorities receive uniform evidence.	Eliminates misunderstandings and mistranslations during international operator-to-operator requests.

The Hop-by-Hop Tracing Model

Step 1: Initiation
An authorised organisation sends a request to the terminating operator (the network that delivered the call to the victim).

- Inputs provided: Date, time (approximate), and called party number.

Step 2: Core Records Search
The terminating operator uses these data points to locate the specific call within their network logs.

Step 3: Upstream Identification
The operator identifies the immediately preceding network operator that handed the call off to them, providing their name, ID, and contact details.

Step 4: Iterative Repeat
The authorised organisation sends a subsequent request to that next upstream operator. This process is repeated loop-by-loop until the originating network is successfully identified.

Leveraging Existing Infrastructure

Why Amend Rather Than Rebuild?

The Foundation:
TS 102 657 is the established technical specification for lawful interception, retained data handling, and handover interfaces.

The Opportunity:
While originally targeted at identifying individuals or organisations via call records and signaling, it serves as a highly useful framework for call tracing.

Key Advantages:
Leverages Existing Systems: Capitalises on data structures and automated processes that network operators have already built and implemented.

Regulatory Burden:
Avoids the lengthy, redundant process of drafting a completely separate technical specification from scratch.

Next Steps & Feedback

The Goal:
Build consensus on whether amending TS 102 657 is the most appropriate regulatory path forward.

ETSI Submission:
Subject to stakeholder agreement, exact structures and formatting proposals will be formally submitted to the relevant ETSI group for standard review. TR will be presented and discussed at the TCLI #73 in Oslo.

Global Integration:
GIRAF have launched a taskforce on Traceback which is led by the FCC within CEPT-ECC-NaN.

Thank you for your Attention!

One Consortium

Know Your Customer Ecosystem Guidelines

Align industry-led standards,
elevate network transparency,
and restore trust in communications

Keith Buell – Numeracle + Leadership Council, One Consortium
Melissa Blassingame – Twilio + Leadership Council, One Consortium

Originating Service Provider's KYC of Large Enterprise

Core Business Details: Legal business name, DBA (Doing Business As) name, business type, industry, and country of registration, Website URL, social media URL, traffic use case

Registration & Tax IDs: Employer Identification Number (EIN) or localized business tax ID.

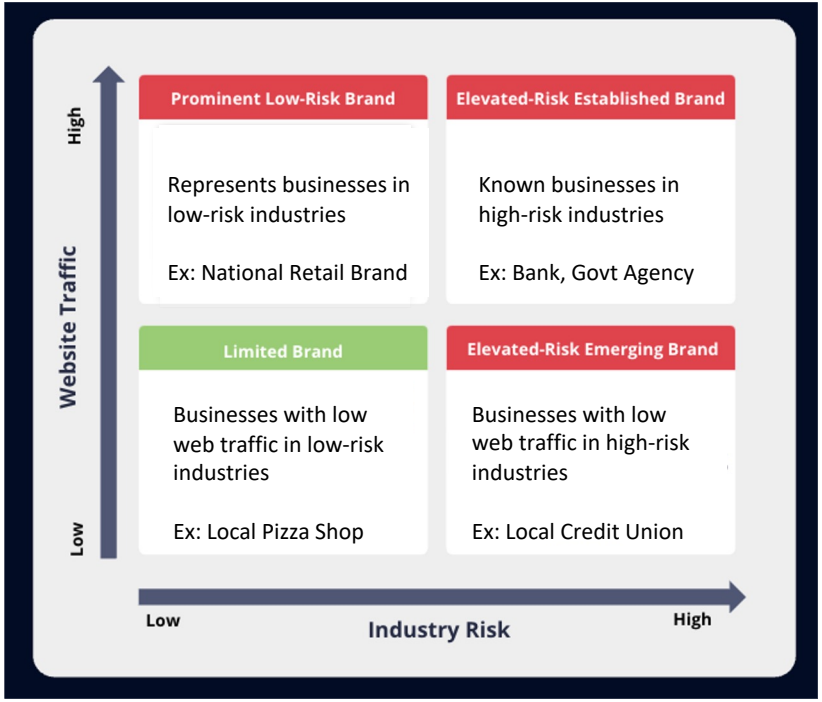
Physical Address: Your exact corporate street address or registered business location.

Authorized Representative: The name, job title, email address, and phone number of an officer or authorized contact (e.g., owner or CEO)

Identity Verification: A government-issued photo ID (e.g., passport or driver's license), live selfie

Risk Tiers: Progressive KYC based on risk signals collected by various platforms and tools

Right to Use: Validate business right to use a brand and its numbers



Terminating Service Provider's KYC of Voice Service Provider

Ownership Details: Name(s), address(es), and email address(es) of all individuals with 10% or more direct or indirect ownership of the company. Determine if the details associated with the prospective communications service provider customer's corporation registration are consistent with the information it has provided about business activities, ownership, legal address.

Sanctions List: Screen the customer, beneficial owners, and parent companies against applicable sanctions and restricted-party lists.

Policies of Customer's KYC: Policy details what the company does to mitigate bad actors and robocall traffic.

Additional Validations: Search for court cases, regulator reviews, and any other news indicative of the prospective service provider and/or owner facilitating illegal or fraudulent traffic. Make enquiries with credit agencies. Ensure service provider adheres to regulatory requirements within country (registration, number disconnects).

Tiered Capacity Access: Impose limits on the service provider's traffic volumes, capacity, or expenditures until traffic profile is proven to be compliant.

Additional considerations and Next Steps

- Vetting must remain adaptive
  - Bad actors continuously subvert rigid, check-the-box regulations. They bypass fixed checkpoints using callback scams, short-lived shell entities.
  - Static checklists become obsolete quickly. Verification guidelines must focus on evolving and adaptive behavior, not static database checks.
  - Modern verification technology is continually evolving to capture far more extensive and rich real-time metadata points.
  - Enforcing rigid, static KYC barriers blocks legitimate customer innovation while failing to deter modern, highly sophisticated AI scams.

- White paper will be published establishing global best practices
  - Objective will focus on vetting large enterprises from the originating service provider and vetting upstream voice service providers from the terminating service provider.
  - Intention is to encourage new service providers to join One Consortium that adhere to best practices and guidelines established.

Spoofing of National CLIs

Cloud Numbers Use-cases
GIRAF Recommendations

Katia Gonzalez - Somos Head of Global Public Policy + Vice-Chair, One Consortium
Thomas Sunesson - Bandwidth Regulatory and Public Policy + Leadership Council, One Consortium

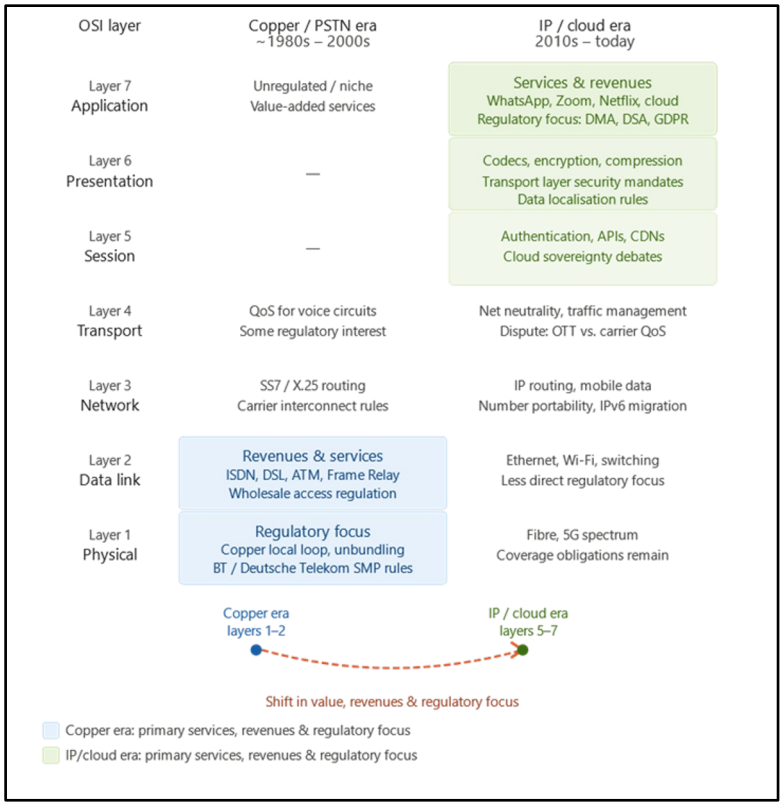
CLI Spoofing

1. National CLIs

- **Roaming** → Whitepaper on Recommendations for legitimate usage validation
- **Cloud Communications** → Whitepaper on Cloud Communications (explanations, use-cases, etc)
- **Cloud Communications** → Whitepaper on legitimate Cloud Communications validation

2. International CLIs

Why One Consortium's work so important?
Market has shifted, regulatory challenges evolving.



In One Consortium, a key focus has been the collaboration to enhance knowledge about the Cloud market.

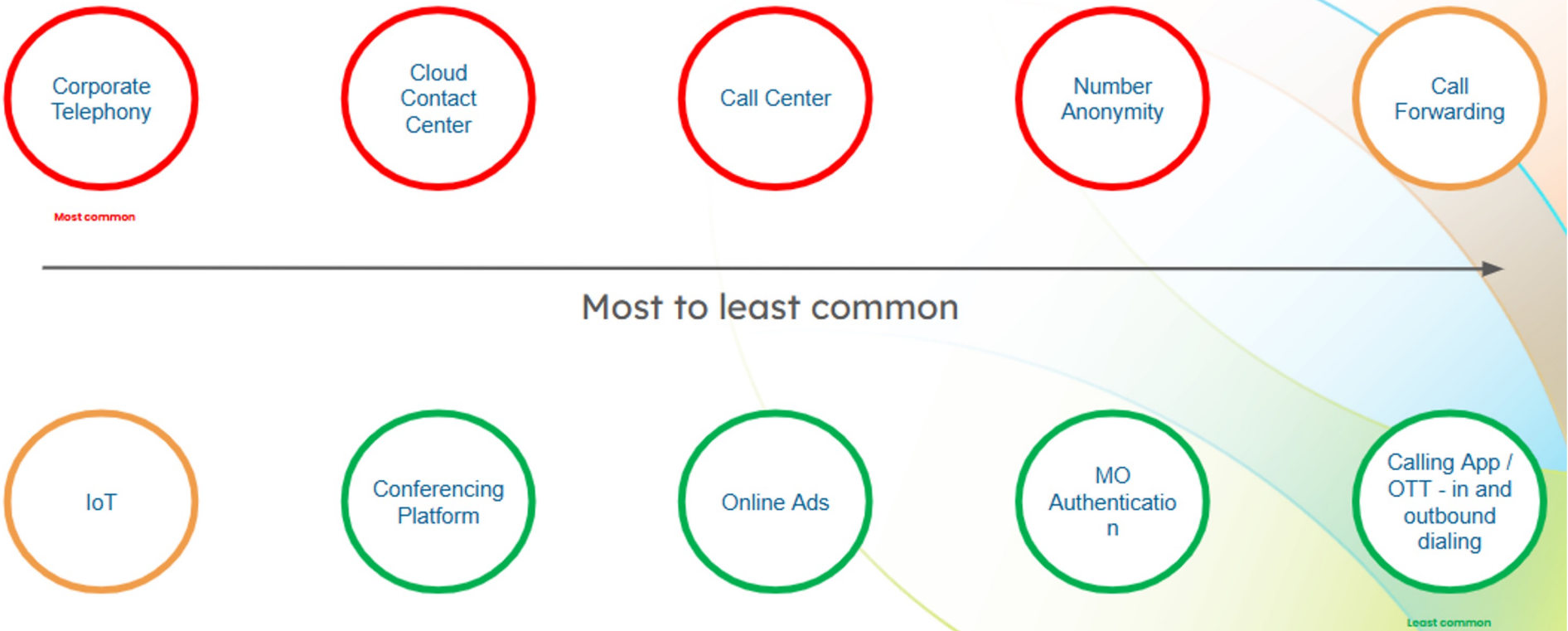
Regulatory frameworks have historically focused on lower layer OSI and on a country-by-country basis.

Today's Cloud technology is cross-border by nature and at higher OSI layers.

Effective outcomes in the fight against fraud and scam => require full understanding of the (cloud) market and these changes. Focus intervention on fraudsters without collateral damage to the important cloud market.

Overview: Use-Cases from the customer perspective (end-user / business)

One Consortium



GIRAF
the global regulatory forum

GIRAF's Recommendations on Spoofing

GIRAF collaborative work is bearing fruit.

On June 8th, GIRAF published its initial Recommendations on Spoofing.

10 recommendations to Telecom Regulatory Authorities to :

- improve the fight against fraud while
- not jeopardizing the handling of legitimate incoming international voice calls or
- not blocking nationally permitted exceptions (ie approved use cases)

One Consortium

What Can We Do As An Industry?

- KYx to Improve Usage Transparency
- Foster Numbering Transparency (eg. on Suballocation)
- Information Sharing
- Right-To-Use and Digital Identity
- Traceback

 Industry Autoregulation vs. Actual Regulation

What Next For One Consortium?

- Recommendations to improve CloudCommunications
- Position vs EU DNA & other public consultations

 KYx, Info Sharing, Right-To-Use, Digital Identity, Traceback

One Consortium

Traceback

initial white paper

Tim French – Wavecrest + Leadership Council, One Consortium
Linda Vandeloop - ATIS + Leadership Council, One Consortium

international traceback : progress to date

a tool for the organizations responsible for fighting unwanted/ fraudulent calls

New paper published with an overview of the landscape

Available on the website at
www.oneconsortium.org/white-paper-international-traceback-high-level-outline/

Topics covered:

- Types of traceback
- Information required and provided
- Suggested operating principles
- Encouraging participation
- Challenges and blockers to adoption
- Governance
- Example global implementations

international traceback : Next steps

a tool for the organizations responsible for fighting unwanted/ fraudulent calls

- Use-case list with one-pager per use case
  - Common use cases and scenarios
  - To cover domestic and international scenarios
  - Requirements, privacy considerations, process management
- Domestic focussed best-practice paper
  - Different models for domestic traceback
  - Pros and cons of each
- Traceback and Privacy paper
  - Privacy as a potential roadblock
  - Mapped onto the use case list
  - Potential solutions to privacy issues
- International Traceback paper
  - Different models for global traceback
  - Mapped onto the use case list
  - Implementation requirements: technical, network, governance, funding

One Consortium

Digital Identity

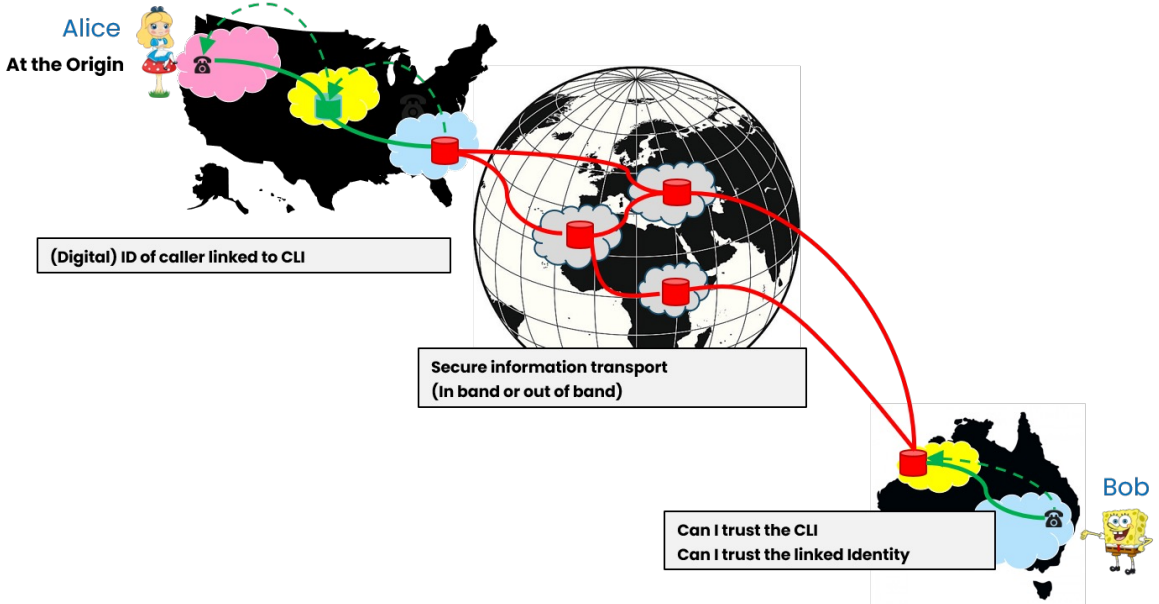
Digital Identity

Who is using the phone number?

Steve Buck – BTS + Co-chair WG6 (with Thomas Sunesson – Bandwidth) + Leadership Council, One Consortium
+ Chair GSMA – Interconnect Fraud & Security

Why Digital Identity is important

- Various mechanisms can ensure **CLI is not changed** (e.g. STIR, call check, national CLI blocking)
- But this **doesn't link the CLI** to the person or business communicating
- The CLI may be unmodified, but communication can still be scam from a bad actor
- Need **CLI to be linked to a verifiable identity** – business or consumer



Elements

IDENTITY	LINKING	VERIFICATION	PRESENTATION
Vetting	**Binding to communication**	**Independent check**	**Trust signal to user**
Multiple vetting schemes, but clarity on scheme and mechanism resulting	In band or out of band certificate associated with communication	Carrier, operator or handset can check identity – what was verified and by whom	Branded display, tone etc

- Allows **national** implementation, but transparency of vetting process and information
- Positive benefit to **encourage adoption** (e.g. Trusted calls answered) not limit existing behavour

- Initial focus **Business to Consumer** (SIP) voice, but with framework that can be re-used
- Working group plans & progress:
  - Introductory whitepaper and powerpoint on solution elements – in final draft
  - Whitepapers on Vetting, Binding and incentives – Q3

One Consortium

Messaging

Initial White Paper

Eli Katz – Xconnect + Leadership Council, One Consortium
Stacy Graham – Sinch + Leadership Council, One Consortium

One Consortium

Restoring Trust across the Global Messaging Ecosystem

The Objective

Create a harmonized framework that enables trust, accountability, and consumer protection across all messaging channels globally.

Roadmap established for:

- Global harmonization
- Cross-industry collaboration
- Stronger consumer protection
- Trusted messaging worldwide

One Consortium

Restoring Trust across the Global Messaging Ecosystem

The Challenge

- Consumers experience messaging as a single channel
  - 📱 SMS
  - 💬 RCS
  - 🌐 OTT Messaging (WhatsApp, Telegram, etc.)

- Each channel operates under different regulatory frameworks, security controls, identify verification requirements and fraud mitigation capabilities

The Result

Fraud follows the path of least resistance!

As protections improve in one channel, bad actors migrate to ess regulated environments, creating inconsistent consumer protection and weakening trust globally.

One Consortium

Key Recommendations and Outcomes

Policy Harmonization
Align expectations across SMS, RCS, and OTT messaging.

Global Registry Alignment
Promote interoperable sender identity and brand verification frameworks.

Unified KYC Standards
Advance consistent KYC, KYB, KYUP, KYT, and identity validation globally.

Traceback and Intelligence Sharing
Enable coordinated fraud investigation across platforms and borders.

Industry and Regulatory Collaboration
Leverage One Consortium and GIRAF to build global harmonization.

Education and Awareness
Equip regulators, industry, and consumers with common knowledge and best practices

One Consortium

Industry and Regulatory Surveys

Restore Trust Resources Portal

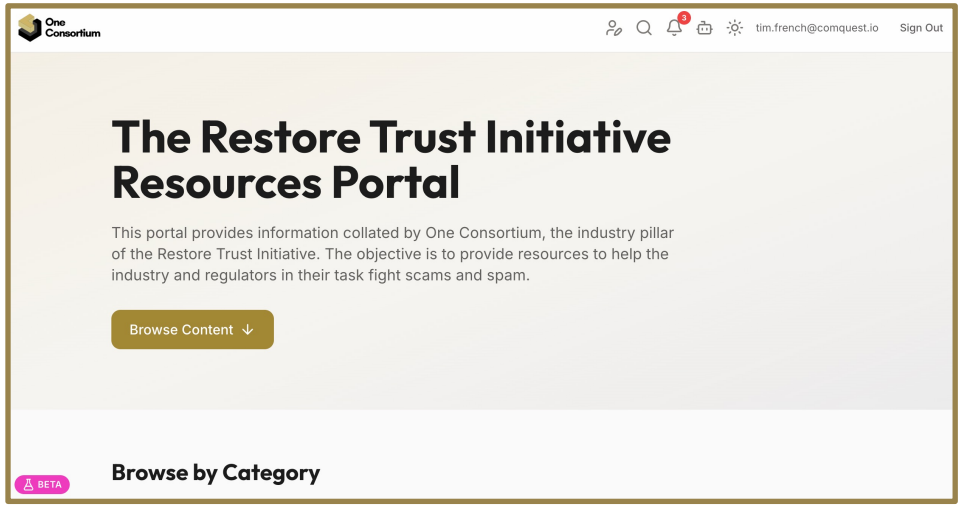
Tim French – Wavecrest + Leadership Council, One Consortium
Keith Buell – Numeracle + Leadership Council, One Consortium

Surveys : Progress update

Surveys of Tools and Regulations to help the industry understand the changing landscape

Initial surveys complete

- Survey of industry tools and best practices
- Survey of regulation (77 countries)
- Now moved to the portal



One Consortium

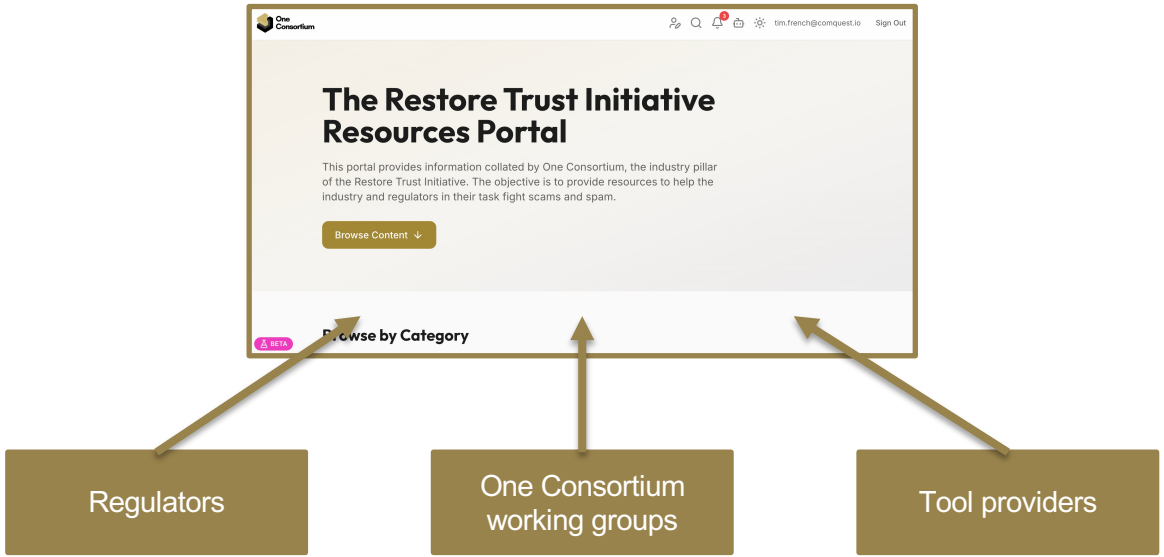
Quick look at that portal

Surveys : Next steps

A tool to curate information to help fight scams and fraud

Move from 'Build' to 'Run mode'

- Add new tools as we become aware of them
- React to feedback, updates and changes
- Allow external parties to add and maintain data on the portal



Restoring Trust
in international communications

Let's join forces!

Join the collaborative work

Review, comment and use One Consortium and GIRAF guidelines
www.oneconsortium.org/publications/

Let's agree an efficient global framework - and drive adoption!

- Telecom Industry , global tech, industry associations
- Telecom Regulators
- Other industries and regulators : banking & payment…
- Law Enforcement
- Policy makers, law makers
- Other private or public initiatives

One Consortium

thank you !

www.oneconsortium.org

One Consortium

Membership
June 2026

Strategic Partners

GASA Global Anti-Scam Alliance

GLF Global Leaders Forum, a techoraco brand

Contributing Members

8x8 · bandwidth · bics proximus · BTS · T · Microsoft · nuso · PCCW Global · consoleconnect · RingCentral · sinch · TATA COMMUNICATIONS · twilio · vodafone · wavecrest · Aegis Mobile · heksagon · netnumber · Numeracle · OCULEUS · PROVENANT · SOMOS · TNS · TransNexus · TransUnion · XConnect A Somos Company

Industry Organizations

atis · CFCA · Cloud Communications Alliance · ctia · COMMS COUNCIL UK · GSC GLOBAL SOLUTIONS COUNCIL · GSMA · i3Forum · INDUSTRY TRACEBACK GROUP · NICC UK Interoperability Standards

Supporting Members

AVISO MESSAGING · COMCAST · colt · iBASIS · identidad Telecom · LUMEN · oni a gigas company · ooredoo · symbio · MTN · 1ROUTE · didXL · Orillion SOLUTIONS · Utel · orange Wholesale