One Consortium

Restoring Trust in Communications

Paris, March 2nd, 2026

One Consortium response to DG Home Call for Evidence on Online Fraud

Restoring Trust in Communications

One Consortium welcomes the opportunity to share our views on DG Home's call for evidence relating to 'Online Fraud'.

One Consortium is a not-for-profit, member funded, member led organization of the global Telecom industry, and the "industry pillar" of the Restore Trust initiative to fight spams and scams globally. One Consortium's 50+ members include Telcom service providers, carriers, and aggregators, global Tech, vendors, and industry organizations such as GSMA, i3Forum, CCA, ITG, CCUK and NICC. One Consortium's objective is to co-develop and drive adoption of a set of recommendations and guidelines to fight scams and fraud, working with the 40+ Telecom regulators from 5 continents who participate in GIRAF, the global informal regulatory forum and the "regulatory pillar" of the initiative.

One Consortium and GIRAF's initial focus is on combating the misuse of voice calls and messages to initiate or commit fraud and scams, from both industry and a regulatory perspective, respectively. An early communication from our forum sets out our challenges and opportunities in re-establishing trust in voice and messaging communications.[1]

As the call for evidence takes a broad approach to 'Online Fraud' and specifically refers to PECN/PECS (Public Electronic Communications Networks/Services), we agree that taking a holistic view on the pan EU anti-fraud steps is warranted: online as well as electronic communications. Please note that all comments submitted by One Consortium relate to the market our members are active in: international voice and messaging, either directly as network providers or resellers or in the associated technology and vendor markets.

We feel that this call for evidence comes at the right time, in the wake of the publication of the proposed DNA which aims to finally establish a truly Single European market and which brings a pan EU approach to tackling fraud in the communications sector within the ODN's (Office of Digital Network) regulatory remit and scope.

In our view, the DNA represents an opportunity to truly tackle Online Fraud in a coordinated, single, and effective manner embracing its international nature; we are also seeing, amongst our members as well as GIRAF a great sense of urgency and desire to combat scam and fraud calling and messaging. Looking at the DNA, specifically, we would like to encourage DG Home as well as DG Connect and the forthcoming Office for Digital Networks (ODN) to take the opportunity of the DNA to establish a harmonized pan EU approach to Online Fraud which approaches the challenges with a clear focus on:

1. Consistency & Harmonization- Achieve legal and regulatory consistency in the fight against Online Fraud across the European Union and with the ambition to seek enhanced consistency on a global basis. Online Fraud is a global issue before it becomes a pan-EU27 issue. Consistency is instrumental in avoiding regulatory loopholes that benefit rogue actors as well as in making sure that one jurisdiction regulations protect both its own and other countries' citizens from being targeted by frauds originated in-country and abroad.

2. Efficiency - Lay down the regulatory framework that enables the industry to introduce actions that target the fraudster in the most efficient manner for the online eco-system. The activity

[1] "Solutions for Restoring Trust in CLI for International Calls" (One Consortium, 2025)

of re-establishing trust in the communications sector commences with giving end users comfort and trust of legitimate and welcome use cases of cloud numbers and then moves onto detecting and blocking malicious activity (including through the use of AI); sharing meaningful information with third parties with the aim of preventing fraud and protecting businesses and end-users and establishing structural cross-sector collaborative procedures.

3. Level playing field - any regulatory measures should focus on the end objective (e.g. fighting fraud) instead of considering the technology channel and means that enable electronic communications (e.g. Voice, SMS, RCS, OTT messaging applications, etc.). Additionally, Online Fraud initiatives should acknowledge and factor in the multiple levels of providing electronic communications services in today's market. Today's communications services are provided by a range of operators that sit at different levels of the OSI table[2], from traditional 'telco operators' to App based communications, and each operator and OSI level has its own technological capabilities and commercial realities that critically affect both the beneficial commercial realities of the communications industry as well as the action and remedies required to combat Online Fraud.

One Consortium views in response to the Call for Evidence:

One Consortium was set up, and is expanding globally - in terms of our members, in terms of establishing a dialogue with law enforcement and others but importantly also in terms of collaborating with telecommunication regulators through GIRAF - in direct response to the global nature of Online Fraud, with our focus being on voice and messaging. We operate and are founded by promoting cross-border and multi-stakeholder cooperation with the focused ambition of preventing, detecting and stopping online fraud as well as identifying fraudsters. We feel we stand the greatest chance to make a real difference to European consumers and businesses as we help drive critical global harmonization and cooperation.

We appreciate the initial breakdown in 8 Problems provided by DG Home, and would like to highlight what are in our view the main priorities, as a global industry organization.

Those priorities can be mapped onto the DG Home's Problem Statements as follows, underscoring where and how One Consortium views and works with GIRAF and other stakeholders, can contribute to the EC's initiative when it comes to calls and messages.

Matrix below describes:

[2] https://en.wikipedia.org/wiki/OSI_model

One Consortium

Restoring Trust in Communications

DG Home: Call for Evidence	Problem 1 Online Fraud through AI	Problem 2 Organized crime & money laundering	Problem 3 Victim support, protection, education	Problem 4 Victims' asset recovery	Problem 5 Public authorities resources, lack of expertise	Problem 6 Collaboration between stakeholders	Problem 7 Private and public sector information sharing	Problem 8 AML
One Consortium			Policy Overlap					
Anti-fraud and industry centric policies for critical resources (Numbering plan, Sender ID…)	✓	✓		✓		✓	✓	✓
Know Your Customer / Know Your Traffic	✓	✓		✓		✓	✓	✓
Traceback	✓	✓		✓		✓	✓	✓
Fight against illegitimate spoofing (alteration of identifiers)	✓	✓					✓	
Information sharing across industry, public authorities and cross-sectors (Banking & Payment etc)	✓	✓		✓		✓	✓	✓
Fraud / scams traffic detection & blocking	✓	✓				✓		
Global harmonization & consistency (industry tools and practices, regulatory and legislative frameworks)	✓	✓			✓	✓	✓	
Global adoption by Telecom and Global Tech, and by Telecom Regulators	✓	✓			✓	✓	✓	
Global cooperation & collaboration	✓	✓			✓	✓	✓	
Information and education of non industry stakeholders (regulators, LEAs…)	✓	✓	Indirect contribution		✓	✓	✓	

As can be seen from the matrix above, we at One Consortium, working with GIRAF and other stakeholders, are extremely active in the remit of this call for evidence and would like to actively engage with DG Home and the wider European Commission in pursuit of an online ecosystem which places restoring trust in domestic and international communications at the heart of legal and regulatory policy. Our work in this area commenced with a thorough and comparative analysis of regulatory regimes, in the EU27 as well as across the globe; a necessity given the global and cross-country nature of Online Fraud (this analysis will be made available in the coming weeks).

Online Fraud initiatives should focus on tackling the root causes of distrust in a collaborative manner, avoid high costs and complexities due to disjointed requirements, and avoid regulatory outcomes that create confusion and delay effective solutions.
In supporting DG Home, we refer to our own focal areas:

One Consortium focus area: "Better control by Regulators and Industry of critical public telecommunications resources". Law makers, regulators and industry must work together to ensure that fraudsters cannot access and misuse such resources.

Online scams and frauds have increased in volume and sophistication in recent years and are now increasingly difficult to detect; both for the defrauded end-user as well as the unwitting communications provider and the other parties involved in the often long, complex and multi-sectoral Online Fraud chain. Technology as well as the use of communications services has changed dramatically in a short period of time; this has introduced a range of new operators to the market and across many different levels which now comprise of 25000 providers in the EU27 alone.[3] These are all positive changes to the market as it drives innovation and delivers real end user value. But these rapid changes, including the shift towards Cloud based communications, have also brought regulatory inconsistencies and shortcomings that cause market inefficiencies as well as enabling Online Fraud. We describe many of the changes, challenges, and opportunities brought on by cloud communications, in general and specifically in relation to Online Fraud in our white paper.[4]

Complexity of the services and of the marketplace and lack of regionally/globally harmonized regulatory and legislative frameworks (across jurisdictions, across channels) also makes enforcement very challenging. Therefore, whilst there are no doubt numerous reasons for the proliferation of Online Fraud, we submit that a key contributor is the past and growing lack of control of critical telecommunications resources.

By way of example:

Numbering Plans:

Apart from “116” numbers, Member States are largely non harmonised in numbering plans and NRAs make available a significant number of different number types (geographic, multiple types of non-geographic, and mobile etc.). The market that these numbers were originally introduced to serve has largely ceased to exist (copper-based point to point calling). All-IP technology used today permits easy ‘use’ of these numbers on platforms they were not originally designed to operate from; this is equally true for benign, as well as malign and fraudulent, uses. It is not difficult to see that end-users are increasingly confused and avoid answering calls caused by this unnecessary numbering complexity.

We are however not seeing that NRAs are making any significant strides to simplify and harmonize these diverging and unnecessarily complex numbering plans, but rather our members raise concerns that NRAs, including all in the EU27, continue to apply divergent and restricting number policies that hamper their commercial roll out of beneficial and modern cloud communications services and divert precious resources from driving growth and combating fraud. Cloud-based voice (including UCaaS, hosted PBX and business VoIP) already represents a significant and rapidly growing share of enterprise voice communications, with double-digit annual growth, while revenues from legacy on-premises systems are on a terminal decline (which the DNA seeks to accelerate). As such, regulatory policies should focus on growing the cloud communications markets and factor in Online Fraud policies based on a forward-looking understanding of the cloud communications

[3] BEREC Authorisation Database
[4] “Cloud Number use cases” (One Consortium, 2025)

market. Holding on to old copper based TDM[5] policies will neither combat Online Fraud nor drive the commercial ambitions of the DNA.

Additionally, in the rapidly growing 'cloud' segment of the communications industry, we are seeing deviating and conflicting definitions being employed across the EU27 and beyond. *Entitlement* to numbers and *use cases* that are permissible (from a cloud platform serving the domestic markets) are drifting apart between NRAs. This creates an uncertain commercial environment for the market segment that should be prioritized by the EU Commission as it adds both complexity to the industry and detracts precious resources to, *inter alia*, the fight against Online Fraud. To enlighten members of GIRAF, we at One Consortium have a dedicated working group looking at the requirements of the cloud industry and have produced materials to help inform the debate; we are of course very happy to share these materials with The EU Commission, including DG Home.

Suballocation:

The commercial model of 'suballocation'[6] [of telephone numbers] has been widely used in the industry for many decades but began to formalize 10-20 years ago (with Spain and Portugal being notable and recent markets where suballocation gained formal recognition and status). Much of the modern, and certainly the innovative, part of the communications industry (VoIP, UCaaS[7] and CPaaS[8]) relies on suballocation of numbers with reasonable market expectations that 40-60% of these modern solutions use suballocations. An entire industry - where these modern and suballocation requiring providers *have not and can not* realistically build out networks of their own and build their commercial offerings has developed on the availability of suballocated numbers.

Today however, we are seeing piecemeal withdrawal of suballocation from the EU marketplace; with Sweden and Greece being recent jurisdictions where it is no longer permissible. However, and with specific relevance to the combat of 'Online Fraud', a recent study by Europol shows that 64% of communications fraud has nothing to do with

[5] TDM (Time Division Multiplexing) voice is a legacy, circuit-switched technology that revolutionized telephony from the 1970s by allowing multiple voice signals to share a single transmission channel via dedicated time slots. It operates using physical switches and copper wires, offering high-quality, reliable connections, but is now being replaced globally by VoIP due to its high maintenance and lack of modern flexibility.

[6] Suballocation in telecom numbering is where an operator that holds primary rights of use over a block of numbers (from the national regulator) parcels out some of those numbers to another provider, which then assigns them to end-users under its own retail or wholesale services. In other words, instead of every service provider having to obtain its own number ranges directly from the regulator, the "rightsholder" can act as a wholesale source of numbers, enabling hosted PBX, VoIP, MVNO, CPaaS and similar models while remaining ultimately responsible for the numbering rights and regulatory compliance.

[7] UCaaS (Unified Communications as a Service) is a cloud-based subscription service that bundles enterprise-grade telephony, video conferencing, instant messaging, presence, team collaboration, and unified messaging into a single, integrated platform accessible from any device, eliminating the need for on-premises hardware and simplifying management for distributed workforces.

[8] CPaaS (Communications Platform as a Service) is an API-driven cloud platform enabling developers to embed real-time communication features—like voice calls, video, SMS, MMS, chat, and WebRTC—directly into custom applications, websites, or workflows without building the underlying telecom infrastructure from scratch.

suballocation. Lack of traceability, transparency and traceability in the number suballocation models, regulatory frameworks and industry practices, might explain why some Regulators take such radical steps, at the risk of jeopardizing legitimate use cases in line with the growth, productivity and innovation goals of the DNA while only improving security to a very limited extent. Whilst we would not condone providing services without necessary Authorization, and without ensuring transparency, traceability and accountability, we can point towards likely outcomes by the regulatory policy decisions being made.

The 2002 [Electronic Communications] Framework, which laid out the foundations of the EECC, drove beneficial competition and consumer protection enhancements but is proving less suitable to combat global Online Fraud.

In today's market, countries or providers that *do* desire to overcome the challenges posed by Online Fraud through the introduction of more stringent requirements or simplifications in the market and thus enable more effective measures against Online Fraud are, from a macro-economic or individual provider perspective, respectively, effectively penalized commercially for such welcome actions. Countries that 'raise' the *de minimis* thresholds of acceptable standards in the fight against Online Fraud see growth developing in other Member States or providers that insist on, say, restricting use cases or applying thorough KYC (discussed below) see contracted traffic, not just fraudulent such, moved elsewhere. This demonstrates that regulatory market incentives are wrong and need a re-fresh and re-alignment.

In conclusion: A successful combat against Online Fraud should include the clarification and simplification of harmonized regulatory frameworks and industry practices regarding numbering in general and number suballocation, develop enhanced, harmonized and clear Right to Use policies, harmonize KYC as well as number verification in order to achieve transparency, traceability and accountability. Moreover, Do-Not-Originate and Do-Not-Call registries are, especially considering the challenges of global cloud communications providers that are operating at a global level and likely lack in country staff with necessary expertise and language skills, are often poorly communicated and at times difficult to find and follow; this may contribute to occasional and inadvertent noncompliance. Tackling these basic steps would also stimulate long-term and sustainable growth in an innovation-centric EU27 marketplace and help harmonize global frameworks and practices. The Digital Networks Act refers, directly or indirectly, to a number of these matters, but we would welcome seeing more concrete steps and suggestions to establish a more certain and cloud communications centric marketplace. We are under no impression that these issues will be resolved swiftly but can offer to DG Home all our internal expertise and collaborative and global efforts on these issues.

One Consortium focus area: "Develop and agree global guidance and a vendor neutral "toolbox" of technologies, best-practices, processes etc. to efficiently prevent, detect, stop and trace unwanted/fraudulent communications (calls and messages) especially when originating from abroad"

Enhance Know Your Customer (KYC) / customer onboarding:
Effective and fraudster targeted measures against Online Fraud should, logically and procedurally, start with effective scrutiny and good understanding of the identity of the customer being invited onto the communications fabric; Identity, location and intended use of

the services requested to be provided represent a *de minimus* set of information necessary for tackling Online Fraud.

However, harmonization of strong KYC requirements across the EU has proven difficult. As an example, despite pre-paid SIMs have been associated with precontract KYC since the 2004 terrorist attack in Madrid introduced KYC in this area, only 19 of 27 EU Member States apply KYC for pre-paid SIM.[9] Outside of pre-paid SIM cards, the EECC remains silent of KYC and the differences across the Member States diverge further.

Our parent organization, i3 Forum, has developed KYC guidelines from amongst their broad range of members[10], and we at One Consortium, based upon our global members expertise and comparative regulatory policy study, are due to publish our own KYC guidelines. Adopting these principles on a wider basis, and establishing effective enforcement thereof, would go some way to establishing a communications market with the right market incentives and creating a strong 'first line of defense' against Online Fraud. We would welcome wide adoption of these principles across the EU27.

Traceback:

Most of DG Home's Problem Statements ultimately depend on being able to track down the fraudster.

In our market segment, this means linking the Online Fraudster (typically the calling party though the opposite occurs as well) to a telephone number (Calline Line Identifier, CLI) and tracing back across multiple networks and countries until the Online Fraudster is localized.

Traceback is a process to identify the true source of the 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 call throughout the call path - traceback can be initiated to determine the path a telephone call takes, potentially through multiple communications networks, and identify the true source of the call.

Working with GIRAF, One Consortium has put together a Traceback document aimed to be a guide for implementing or 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 many 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. We would be delighted to share our findings in this area with DG Home.

---

[9] "19 EU countries mandate the registration of prepaid customers" (Cullen, 2025)
[10] "Principles and best practice for mitigating fraudulent, illegal and unwanted communications" (i3 Forum, 2025)

Restoring Trust in
Communications

‘Spoofing’:

Telephone numbers originated at a time when networks were copper based and therefore had a high degree of ‘built in’ fraud protection; these days, phone numbers are operating from cloud-based platforms and can very easily - for beneficial as well as detrimental purposes - be manipulated. A recent study by Europol shows that 64% of communications fraud is linked to this detrimental practice of illegal CLI manipulation (“Spoofing”) and we understand the wider concept of ‘Spoofing’ or impersonation is a concern also under the Payment Services Directive and Regulation. It is prudent to expect that Online Fraud through spoofing will, unless combated collaboratively and on a cross-border basis, rise dramatically in the near future. A key focus within the communications industry, and the central reason for One Consortium to come together, is how to re-introduce trust in international calls and messages.

Whilst we are technologically neutral on *how* the industry can deliver trustworthy identity markers (the presented telephone number) to the receiving calling party, the most well-known technology, STIR, has, *inter alia, been* introduced in France (locally known as “MAN – Mécanisme d’Authentification des Numéros”). Another solution is Cross Border Call Authentication, CBCA. Cross-border call authentication expands STIR frameworks internationally to verify caller ID authenticity, reducing spam/robocalls on global, incoming, and outgoing calls. It facilitates interoperability between national STIR frameworks (e.g., France, U.S. and Canada) by allowing sharing of vetted service provider lists and certificates, enhancing trust in international voice communication. CBCA is an industry led initiative managed via ATIS. Other solutions are also emerging across the industry.

Though the technologies that can be employed to enhance end user trust in the identity of a caller are yet to be determined, we are certain that the most effective solution will be established and delivered by the industry working collaboratively at all levels and across borders.

To help our members as well as GIRAF navigate through the challenges of evolving technology whilst remaining focused on delivering enhanced trust in a commercial and competitive marketplace, we recently expanded our focus to also include a Working Group on ‘Identity’. Whilst a relatively new working group, we lean into previously completed comparative analysis of regulatory practices across the globe as well as benefitting from vast experience, across all market segments and technologies, that our members bring. We expect material developments from this working group in 2026 and would be delighted to share with DG Home as well as GIRAF our findings and recommendations.

One Consortium focus area: “Pursue global harmonisation across jurisdictions and level playing field across channels, and foster collaboration between industry and all stakeholders that can deliver trust in the communications market.”

In this short paper, we have highlighted some key areas where we would welcome DG Home to draw its attention to. From poor and disjointed use of critical resources to slow and piecemeal implementation of tools and processes. Focusing on these would allow the industry to take the lead on combating Online Fraud.

Though the main message here is to collaborate widely and across borders, a specific matter worthy of mentioning is the impact of European Data Protection rules. We have experience, both individually and as a member of several industry bodies, that there exist concerns around 'sharing of data' within the industry. This concern often results in no data being shared at all and the existence of suspicious communications traffic is not flagged to other communications providers who are either in the communications chain of that suspicious traffic, or likely to 'pick up' the traffic if the first provider shuts down the fraudulent dialler. Whilst sensitivities around sharing of data is ultimately wise and likely a strong indicator of how important general Data Protection is within the industry, the very same 'merits' are now, possibly, making it more difficult to combat Online Fraud.

In addition to the critical workflows outlined in earlier sections, we believe however, as did the Swedish government[11], that fraud and scam must be tackled at a cross-EU level, and beyond, in a consistent, targeted, efficient and even playing field manner. In fact, we hold the view that the former represents a *de minimis* position; fraud is a global affliction that lives off regulatory imprecision and technological opportunities at a global scale. DG Home, working with DG Connect and external stakeholders, now has the opportunity to establish a collaborative environment, including in the set-up of the ODN, with a view of tackling these challenges. The EU is also well positioned to lead the global enhancement and harmonization of frameworks and practices, working with all stakeholders. This is a critical aspect of the fight against fraud and scams, a $1 trillion USD global threat that calls for a global response.

Online Fraud can however not be combated in a manner that ignores the goals of the commercial industry that online fraudsters misuse. We therefore ask DG Home to continue to collaborate widely and proactively seek the views from the many industry participants, many of whom we represent at One Consortium, so that an industry and expertise led solution can develop quickly, cost effectively but also on terms that allow the modern communications industry to continue to grow and deliver tremendous end user value for the European citizen as well as Member States in general. Fighting fraud in isolation or devising solutions without the input from industry players will not accomplish a reduction of Online Fraud on the market but would deliver extensive collateral damage to the nascent and fragile competitive cloud communications market.

We strongly welcome DG Home to reach out to us at One Consortium for a holistic and outcomes driven discussion in the collaborative fight against Online Fraud.

For One Consortium,

Philippe Millet

Founder and Chairman of One Consortium

[11] "Cyber fraud should be combatted at the EU level. To be able to respond to current and future methods of fraud, legislation with the purpose of addressing misuse of electronic communications services should be proposed that is flexible and future proof." From: "Non-paper: Sweden's key messages and proposals for the Digital Networks Act" (Swedish Government, 2025)