Consultation response form

Please complete this form in full and return to CLIauthentication@ofcom.org.uk

Consultation title	**CLI authentication: a potential approach to detecting and blocking spoofed numbers**
Full name	
Contact phone number	
Representing (delete as appropriate)	Mobile Ecosystem Forum
Organisation name	Mobile Ecosystem Forum (MEF)
Email address	

Confidentiality

We ask for your contact details along with your response so that we can engage with you on this consultation. For further information about how Ofcom handles your personal information and your corresponding rights, see Ofcom's General Privacy Statement.

Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential? Delete as appropriate.	Nothing
Your response: Please indicate how much of your response you want to keep confidential. Delete as appropriate.	None
For confidential responses, can Ofcom publish a reference to the contents of your response?	Not Applicable. There are no confidential responses

General Remarks:

The Mobile Ecosystem Forum (MEF) is a global not-for profit association established in the year 2001 to advance and protect the potential of mobile communications. Our members offer multiple perspectives in the ecosystem including mobile network operators, connectivity providers, wholesale vendors, security solutions, system integrators, content providers, financial players, and retailers. MEF headquartered in London, UK, with subsidiaries Brazil and Ireland.

- **The Mobile Ecosystem Forum (MEF) supports and welcome all efforts to limit fraud and protect the end consumer. The industry can limit threats, but it should do more and increase speed of its responses**.
- **MEF believes that there is no single technology that can deal with text and call spoofing. MEF supports CLI authentication, especially to protect consumers from fraud.** Focussing on a single solution is potentially detrimental for the end user. A concerted effort to react and respond

quickly to threats is more likely to fend off the multiple systemic attacks attempted by fraud-sters.

- **The implementation of STIR alone would not stop spoofed calls. STIR is a valuable tool for building trust in Caller ID for voice calls,** but it is not a silver bullet for reducing scam calls. It is still important to be vigilant and use other tools to protect yourself from fraud, see the U.S.A. data. In addition, STIR would not cover text-based threats, allowing for displacement of fraud from one channel to another. The regulatory response should articulate the problem across the channels, and not with reference to one only.
- **If STIR were to be rolled out, we could suggest adding further elements to the CLI authentication solution such as**:
    - Increasing focus on establishing identity of callers, not just authenticating transport carriers
    - Actual meta data on calling party.
    - The use of a central numbering data base since the ability to traceback is important to fight bad actors.
- **Blocking or disrupting calls is not the only potential answer to spoofing. 'User Guidance Indicators' could provide an important defence mechanism, and trust enhancing feature. This is a long-term solution to be developed with the wider telecom ecosystem, but one that could qualitatively improve the customer experience** It is possible to increase user confidence on the authenticity of the caller by first establishing identity and sharing identity attributes with the end users.
- MEF encourages Ofcom to establish goals and outcomes for the industry to work towards, rather determining tools to be applied. **We encourage Ofcom to establish accountability in the industry and establish the positive outcomes it wants to see in the market. These should reflect the user experience and not just the roll out of a single specific technology – which might not by itself have an impact.**
- **We recommend an approach including more flexibility to responds and plan to threats as they develop over time.** We believe the UK needs a forum for the industry to consult and respond in near real time to the emerging threats, sharing information, proposing responses. The UK Sender ID Protection Registry is a positive example for SMS spoofing, and it has now been copied globally. For disclosure, MEF chairs this forum in its role of secretariat, but the overall model could be used in this context.

Your response

Question	Your response
Question 3.1: Do you agree with our analysis of the ways in which number spoofing is used, and the extent and types of harm associated with its use? If you have any further evidence which demonstrates the extent and types of harm involved, please provide this.	**The threat of number spoofing is real and troubling for the entire industry, as it erodes trust in the whole telecom service.** Unfortunately spoofing has already resulted in significant damage to the market. Short-term action is essential to address the challenges we face (2024). A long-term plan may be too late, as the situation may have changed by then. We need to be agile and responsive to the needs of the moment. Consumer Trust in telecommunication services is threatened by the volume of fraud. In the **2023 MEF Consumer Trust Survey,** British smartphone users reported receiving unsolicited text (44% of them, vs. global average of 49%), unsolicited calls (43% vs. global average of 48%), reported receiving fraudulent text messages (37% vs. global average of 39%). Despite the challenges, UK consumers are more confident in their ability to stay safe. The consumer trust index showed a (+4% p.p. year on year) increase in confidence with consumers believing safety from threats is improving. In the United Kingdom, incidence of unsolicited texts remained stable year on year, but unsolicited calls dropped year on year by 2 percentage points, incidence of fraudulent text messages dropped year on year by 7 percentage points. The improving trend is consistent with the previous year benchmarks. **The UK telecom industry has made significant progress in limiting threats to consumers.** This is a testament to the actions and successes of the industry, which should be encouraged and supported. The UK Sender ID Registry has significantly reduced the success rate of fraudsters attempting to use alphanumerical aliases in the SMS network. This UK development has been exported to other countries, and its approach could provide important learning for spoofing prevention efforts around the world.
Question 4.1: Do you agree with our assessment that while Ofcom rules and	MEF agrees that more needs to be done to tackle number spoofing. This is a complex problem that requires shared accountability and clear lines of

industry measures are likely to help to reduce scam calls, more needs to be done to tackle number spoofing? Provide reasons for your answer and include any suggested measures that could have a material impact on reducing the incidence of scam calls involving number spoofing.	action. A single solution is unlikely to be effective, and no single decision will significantly limit the actions of fraudsters. Fraudsters are becoming increasingly adept at adapting to new challenges, so the industry needs to be able to manage both long-term solutions and short-term tactical responses. Coordination, responsiveness, and information sharing are essential principles that should drive all activity in this area.Attestation by itself is not likely to reduce the volume of fraud calls. STIR is a valuable tool for limiting CLI spoofing in parts of the networks, but it is not a panacea. It is important to consider the empirical results in other markets such as the USA and Canada where volumes of fraud were displaced from purely domestic routes to international ones, or from 'protected routes' to 'non-protected routes.' Unless STIR is mandated universally in telecom networks it is likely that fraudsters will find weaker points to exploit. There are several complementary solutions to STIR, such as in-band and out-of-band implementation of additional header data, a central phone number registry, and phone number verification solutions based on existing data sets. Multiple types of solutions are currently offered or used by MEF members. The industry should not limit itself to STIR alone but should continue to deploy and devise new solutions to tackle number spoofing. DNO lists and CLI validation against numbering plans are good foundational requirements. CLI attestation and validation using STIR are also valuable tools. However, MEF recommends extending validation requirements to include additional data sets, such as assignment or fraud reports. An industry forum to align and orchestrate different fraud responses is more likely to have an impact. Fraudster strategically attempt to change their attacks. The positive experience of the UK Sender ID Protection Registry, an anti-smishing registry set up by UK Finance, Mobile UK, the UK National Cyber Security Centre, and the Mobile Ecosystem Forum provides a reference for such a platform. Originally aimed at managing a registry it developed into a forum for information sharing, joint activities, and rapid escalations.

Question 5.1: Is the approach to CLI authentication we have outlined feasible and workable?	*Is this response confidential? – Y / N (delete as appropriate)*
Question 5.2: To what extent could adopting this approach to CLI authentication have a material impact on reducing scams and other unwanted calls? If you consider an alternative approach would be better, please outline this and your reasons why.	STIR is not likely to reduce spam or unwanted calls. The USA example is a good reference point. Since the introduction of STIR the consumer experience has decreased. YouMail robocall index (https://robocallindex.com/) has reported the USA number of robocalls (i.e., SPAM calls). This index has increased from less than 4 billion a month in 2021 to over 5 billion in May 2023. STIR/SHAKEN has not been able to limit the impact to consumer in the USA, the volumes of calls have significantly increased. This is not to say that STIR is not a valuable tool, but it shows how fraudsters could be using the implicit vulnerability and predictability of the solution to implement successful strategies. CLI authentication is a critical step in building trust in phone calls by helping terminating service providers and consumers identify authentic calls. It is important to note that STIR/SHAKEN has been extended to non-IP networks to further this goal, the solution is evolving for better support. MEF supports the suggestion of creating in UK a common numbering database could play a role in CLI authentication among other services. This is line to international experiences. International traceability of calls from gateway would represent a challenge and potentially eroding real connectivity. This area seems particularly at risk for fraudsters attacks, increasing complexity for good industry players. The “Openness of Communications” should not be at risk.
Question 5.3: Are there additional measures that could be adopted to further strengthen the suggested approach and/or minimise the identified exemptions?	*Is this response confidential? – Y / N (delete as appropriate)*

Question 6.1: Do you agree with the approach outlined for the monitoring and enforcement of the rules with regard to CLI authentication? Are there any alternative approaches that we should consider?	*Is this response confidential? – Y / N (delete as appropriate)*
Question 6.2: Do you agree that CLI authentication could make call tracing easier and yield benefits in terms of detecting scammers and nuisance callers?	*Is this response confidential? – Y / N (delete as appropriate)*
Question 7.1: What are your views on the timescales for the potential implementation of CLI authentication, including the interdependencies with legacy network retirement?	*Is this response confidential? – Y / N (delete as appropriate)*
Question 7.2: Do you agree with our assessment of the administrative steps required to implement CLI authentication and how these should be achieved?	MEF supports the idea of the Administrator role, however we believe that the nature of the work of the administrators will require the separation withing the Administration of two separate functions: 1- Solution. Managing of the Operational Activities and underlying platform the running and functional implementation of the solution. 2- Secretariat – an industry body/forum to manage governance and reporting, including: a. The awarding of contracts for the operational activity to a solution management organisation b. Creation, discussion, and improvement of rules and regulation c. Sharing of information to industry players d. Reviewing of operational activities performance and KPIs e. First escalation of infringements or irregularities 3- Supervisory reporting – the controlling the overall effectiveness of the solution and potential final escalation. This would allow to separate functionality of the technical solution vs the industry, and the role of

	the regulatory input. Such a model has been used in the setting up of the UK Sender ID Protection Registry, and it has provided a good governance model.
Question 7.3: Should a common numbering database be implemented to support the CLI authentication approach? Please provide any comments on the steps needed to implement a common numbering database, including on the feasibility of the industry leading on (a) the specification; and (b) the implementation?	SMS spoofing is mitigated in the United States by the industry's adoption of a common numbering database (CNDB). This database distributes unequivocal and transparent information on the allocation of phone numbers to service providers, allowing all messaging ecosystem participants to block sender IDs from unauthorized connections and bad actors. The regulator should set up the CMDB framework as an essential part of the activity of consumer protection, even outside the planned STIR solution. The establishing of the rules, operators, and solution of this are important to be managed by Ofcom directly - a view to support transparency, accountability, and fair competition in the market.
Question 8.1: Do you agree with the proposed framework for impact assessment and the potential categories of costs and benefits? Please identify any other factors that we should take into account in our assessment.	*Is this response confidential? – Y / N (delete as appropriate)*

Please complete this form in full and return to: **CLIauthentication@ofcom.org.uk**