FCS response to Ofcom's CLI authentication: a potential approach to detecting and blocking spoofed numbers consultation - June 2023.

Introduction

The Federation of Communication Services represents companies which provide professional communications solutions to business users. Our members deliver telecommunications services via mobile and fixed line telephony networks, broadband, satellite, wi-fi and business radio. Our members' customers range from SMEs, home-workers and micro-businesses up to the very largest private enterprises and public sector users. FCS is the largest trade organisation in the professional communications arena, representing the interests of circa 350 businesses which supply B2B services nationwide.

Federation of Communication Services

Website: www.fcs.org.uk
Unit 14, The Stottie Shed, Baker's Yard, Christon Road, Gosforth, Newcastle upon Tyne, NE3 1XD

The Federation of Communication Services Limited
Companies House Reg. no. 2749617
VAT No. 611 911 473

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)	Organisation
Organisation name	Federation of Communication Services (FCS)
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?	Yes

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.	*Is this response confidential? – N* *FCS understands/agrees with Ofcom analysis of the ways in which number spoofing is used, and the extent and types of harm associated with its use.*
Question 4.1: Do you agree with our assessment that while Ofcom rules and 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.	*Is this response confidential? – N* *FCS agrees with Ofcom's assessment that while Ofcom rules and industry measures are likely to help to reduce scam calls, more needs to be done by industry to tackle number spoofing.* *FCS members have highlighted the fact that spoofing machines/software, that they know is used by spoofers, is openly available on the internet and ask whether it should be? One example of many is highlighted here https://www.imyfone.com/change-location/best-call-spoof-app/*
Question 5.1: Is the approach to CLI authentication we have outlined feasible and workable?	*Is this response confidential? – N* *FCS believe the Ofcom approach to CLI authentication outlined is feasible and workable but only if the correct expert industry governance body is put in place to take a lead role on delivery. The funding mechanism must also be assessed and agreed at an early stage, this has been a weakness and delaying factor in other industry wide projects and programmes previously and must be in place early.* *There must be a holistic, not a siloed approach to spoofing reduction. This should include CLI authentication, Centralised Data Base, number management, allocation of numbers and*

	monitoring of number usage. Ofcom must effectively control overall number management. CLI authentication will not be very effective in isolation and will only become fully effective if an industry managed Centralised Data Base (a master central number management and routing database used by all carriers) is implemented, together with a well controlled number management system (with real time authorised porting and reverse look up plus allowed IP lists for regulated/registered carriers). Successful CDB implementation is critical to the holistic approach that the FCS proposes and supports. *FCS believes that in the All-IP world, industry/we should be able to verify where traffic comes from and ensure that only "safe" information is allowed to pass.*
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.	*Is this response confidential? – N* *FCS believe implementing CLI will have a considerable material impact on reducing scams and other unwanted calls but only if done correctly, with industry support and empowered governance and only if an expert, dedicated 'CLI Authentication Administrator' team is put in place, together with the CDB implementation in parallel.* *Industry is aware that whatever authentication is put in place, people will continue to try to operate in a fraudulent manner. FCS believe that continued and empowered industry governance will need to be in place to assess fraudulent activity and agree action needed from an industry wide perspective. The industry governance would work closely with and report into Ofcom.*

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? – N* *There will continue to be both technical and regulatory risks, especially where manual interventions are required. Therefore FCS supports empowered industry governance to continually assess fraudulent technical activity, working closely with Ofcom who can tune regulation appropriately to cover persistent serious infringement types and take enforcement action, where required.*
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? – N* *FCS agree with the approach outlined for the monitoring and enforcement of the rules with regard to CLI authentication but feel that rigorously controlled Ofcom standardised 'onboarding to CDB' governance must be in place. This governance would ensure that each CP is properly onboarded and agrees to follow specific rules. It should also have holistic oversight, monitoring for and identifying serious persistent infringements/infringers. There should also be an overarching (high level) industry project plan, supported by Ofcom that will provide the required strategic steer.*
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? – N* *FCS agree that if implemented correctly, CLI authentication could make call tracing easier and yield benefits in terms of detecting scammers and nuisance callers, enabling appropriate Ofcom and CP action to be progressed.* *While CLI authentication may make call tracing easier, it is essential that the Communications Provider has not been the victim of a 'passing off fraud' and that the details held by the CP relating to their end-user are genuine. A legitimate and authenticated CLI is traceable, but if the*

	user of it has obtained the CLI fraudulently and is not who they claim to be, then the calls could continue until the CP is advised and required to suspend their service. In this scenario, when calls are blocked the scammers could then impersonate another business or individual, obtain new CLIs, and begin calling again. Proof of identity for obtaining telecoms services needs to be tighter if this type of activity is to be prevented or at least reduced, particularly in the All-IP world where geographical linkage to CLIs no longer exists and services do not need to be connected to premises but only to a device. CLI authentication is only one layer of defence and the holistic approach should include appropriate verification of the end-user by the CP. *FCS feels that while 'single level CLI authentication' will be positive progress and goes some way towards reducing spoofing, forensic Ofcom/industry analysis and assessment of what multiple factor authentication will be required to actually 'stop' spoofing will be required. Once more fully understood, the correct multiple levels of authentication can then be assessed, costed and where agreed, implemented. The holistic integrated multi system approach, including CLI authentication, CDB, number management and others (number porting for example) will work towards enabling effective multiple authentication.* *If in future, mobile numbers end up in the CDB, early planning will be required together with security due diligence with respect to the numbers.*
Question 7.1: What are your views on the timescales for the potential implementation of CLI authentication, including the	*Is this response confidential? – N*

interdependencies with legacy network retirement?	*FCS believes that CLI authentication in 2025 is practical to align with the move to All-IP. However, for this to work effectively, holistic planning needs to start now. Funding and governance principles need to be agreed together with an overarching 'high level' project plan, which considers the inter-related overall industry requirements.*
Question 7.2: Do you agree with our assessment of the administrative steps required to implement CLI authentication and how these should be achieved?	*Is this response confidential? – N* *FCS is generally supportive of the proposed steps but an industry agreed 'high level' programme delivery plan with underpinning dates for key interdependencies needs to be in place prior to 2025. Ofcom should also consider entrant establishment onto CDB, ensuring effective and robust CP onboarding and validation.* *Ofcom may need to progress a number of consultations on the inter-related areas, to enable the holistic capture of all considerations that then need to be planned and implemented by industry with Ofcom support and oversight. Ofcom should also take learning from the current switching implementation experience, where no funding mechanism was agreed, it was left to industry to progress with little initial governance agreed and there has been no high level plan agreed or supported by Ofcom to ensure successful implementation.*
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?	*Is this response confidential? – N* *FCS has long supported the implementation of CDB together with associated essential industry agreed governance and an agreed cost model. FCS believe that with appropriate Ofcom support, industry governance can agree funding, put in place an implementation*

	programme plan, deliver CLI authentication together with the mandatory CDB. Ofcom must retain number management and allocation (and could for example charge for number allocation to help fund the holistic changes required) and also rigorously control CDB onboarding.
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? – N* *FCS supports the proposed framework for impact assessment and the potential categories of costs and benefits.* *In addition, FCS would propose an empowered industry governance body to continually assess fraudulent technical activity, working closely with Ofcom who can then tune regulation where required to cover persistent serious infringement types and also take enforcement action, where appropriate.* *With respect to other ideas to help address CLI misuse, FCS would ask if there is any formal obligation on a CP to provide a contact which can be shared with all CPs with respect to sharing of suspect CLI data? Understanding there is a certain level of confidentiality with this, but FCS is aware that some providers already collaborate when certain suspected CLIs start generating spam/scam traffic. Could a facility be considered for CPs to report or receive from a central point any suspected activity together with a named contact at each CP for progressing/collaborating and who could also meet (online) monthly to analyse behaviour and help weed out repeat offenders.*