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* Yes, agreed. No further evidence to add.
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* Yes, agreed. More needs to be done, as evident by the prevalent instances of caller ID spoofing scams happening in the UK.
Question 5.1: Is the approach to CLI authentication we have outlined feasible and workable?	*Is this response confidential? – N* It remains unclear if the proposed approach to CLI authentication is feasible and workable. First of all, the definition of "authentication" in this consultation document seems to be different from the conventional understanding of "authentication" in security. The proposed "CLI authentication" approach is essentially the same as STIR/SHAKEN. However, calling it "CLI authentication" is inaccurate, since the authentication is performed based on the exclusive possession of a secret signing key held by a carrier. Hence, the proposed approach authenticates the "carrier", not the "CLI". We think it is important to clarify this difference, as it is fundamental, and is related to the root cause of several limitations associated with the proposed approach. Second, the outlined approach critically depends on an "administrator", who serves the

	same role as the certificate authority (CA) in a public key infrastructure (PKI). It remains unclear how this administrator will be chosen and managed. From 5.25, “we would expect this entity [Administrator] to be a body of which all UK providers would be members”. This cannot work. Here, the administrator (or CA) works as a “trusted third party”. All providers must trust it and also pay it for the issuance of digital certificates (in the US, the fee is normally based on each provider’s annual revenue). If all UK providers are “trusted third parties” for themselves, there will be a clear conflict of interest. Third, expecting the originating provider or the international gateway to fully attest if a caller is authorized to use a number without having the relevant cross-provider user information is not realistic. From 5.29, “If the originating provider is unable to satisfy themselves about the legitimacy of the numbers being used, they must not attest that call”. In fact, if the originating provider is unable to satisfy themselves about the legitimacy of the numbers being used, they must not originate the call in the first place. This would have significantly reduced the spoofing problem without using the proposed approach (or STIR/SHAKEN). However, the originating network has no incentive to do this as that will cause them a loss of revenue. Imposing regulation on the originating network might help but is unlikely going to be effective due to the fact that the originating network provider does not always have the knowledge - or a well-defined procedure - to judge if the caller is authorized to use a number especially when the number is controlled by a different provider. The proposed “CLI authentication” tries to address this problem by introducing a common numbering database, but details of this database are lacking.
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* The impact of the proposed approach on reducing scams and other unwanted calls is unclear. The accompanying document “Issues in calling line identification (CLI) Authentication in

	the United Kingdom based on the Experiences in North America" prepared by Richard Shockey in June 2021 in support of the adoption of STIR/SHAKEN in the UK is out of date. It must be updated to include up-to-date metrics and assessments to demonstrate the effectiveness of STIR/SHAKEN based on its real-world deployment in the US and Canada from 2021. We suggest Ofcom consider an alternative approach called Caller ID Verification (CIV), which authenticates the caller ID based on challenge-response rather than a digital signature. The CIV solution is detailed in the recent 2023 paper "Spoofing Against Spoofing: Towards Caller ID Verification In Heterogeneous Telecommunication Systems" (https://arxiv.org/ftp/arxiv/papers/2306/2306.06198.pdf). Reasons as to why this alternative approach would be better include: 1. It does not require a trusted third party (namely, the administrator). 2. It works for both IP and non-IP networks. 3. It can increase a telco's revenue if CIV is implemented in the Telco's cloud as a new service that users can subscribe to. 4. If it proves to work in the UK, it can provide a portable solution to sell to Telcos in other countries.
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* Nothing to add.
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* We don't agree. There is a clear conflict of interest for UK providers to be the "administrator" to enforce infringement conducted by the providers themselves. From 6.18, "We envisage that in such circumstances, the membership rules might

	allow the Administrator to suspend or expel non-UK providers from membership in the event of serious non-compliance, to protect the integrity of the CLI authentication regime.” We are concerned that UK providers will have the power to suspend or expel non-UK providers through the “administrator”. This can be detrimental to competition, and there is a clear conflict of interest for UK providers to be law enforcers here. We propose that Ofcom consider the alternative CIV approach (see our response to Question 5.2) that does not rely on a trusted third party.
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* It does not necessarily make call tracing easier. First of all, it will not help trace calls across borders unless all overseas providers accept the “administrator” as their root of trust and are willing to pay annual certificate fees. Second, attackers always exploit the weakest link in the chain. One weak link is key management. As providers are mandated to digitally sign calls, they must securely manage their private keys. The best practice is to use Hardware Security Module (HSM) to manage crypto keys, but HSMs are very costly. When private keys are managed in software, the risk of key exposure increases. A stolen private key may be used to sign arbitrary calls. When a private key is compromised, it must be revoked in a public list, but managing and distributing the list of the revoked keys in a timely manner can be a complex problem on its own.
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? – N* We don’t have particular views on the timescales but would like to highlight that if any part of the call path traverses a legacy network, the whole digital signature will be dropped. Hence, it may require “all” of the legacy networks to be replaced by the IP networks, rather than the “vast majority” for the proposed solution to work. This implies a

	timescale significantly later than “the end of 2025”. By comparison, the alternative CIV solution doesn’t require 100% adoption to be effective, but it does need to get adoption by some of the main telcos to get critical mass.
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* We don’t agree with the assessment. We don’t think the outlined administrative steps can effectively implement CLI authentication. From 7.9, “Our expectation at this stage is that these would be matters for telecoms providers to seek to agree collectively.” The administrator is the root of trust for the proposed “CLI authentication”. Every provider will want to be the root of the trust as that gives them not only administrative power over others but also lucrative financial gains as every other provider must pay them for the issuance of digital certificates. There is clearly a conflict of interest for telecom providers to decide who should be the root of the trust of all providers.
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* To support “full” attestation (Level A attestation in STIR/SHAKEN), a common numbering database seems necessary to provide the originating network or the international gateway with the relevant information to decide if a caller is authorized to use a caller ID. Inevitably, this database will contain information about which users own which phone numbers across different network providers. This information is commercially sensitive and is potentially harmful to user privacy. The key questions are: 1) who will maintain this database, and 2) who has access to it? It seems every provider involved in the CLI authentication framework will need access to this database. This will raise serious privacy/secrecy concerns for the user as well as for the provider.

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* We broadly agree with the proposed framework, however, we should stress that the proposed CLI authentication approach (STIR/SHAKEN) is not the only possible solution. for example, CIV is an alternative solution. Therefore, we propose that the second consultation should include an assessment of CIV in comparison to STIR/SHAKEN. Other factors that should be taken into account: ● Under Objective 3 (8.18), the cost of managing private signing keys is not considered. The industry's best practice of key management requires the use of Hardware Security Modules (HSMs), but that will drive up the cost significantly. ● Other adverse impacts (8.21): the substantial investment required in the management of private keys and digital certificates in compliance with the public key infrastructure may drive small VoIP providers out of business, hence harming competition.

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