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? – No* Colt agrees with Ofcom's analysis and the extent to which number spoofing is used. Phone number spoofing, as well as spoofing over VoIP, has become increasingly popular in recent years. The adoption of IP has given fraudsters an attractive attack vector, with around 45% of fraudulent calls made using VoIP lines. However, as enterprises and technology have collaborated to improve digital defences, fraudsters have moved into the riskier world of social engineering in order to gain access to phone systems. Colt has experienced an increase in the number of requests for assistance addressing voice fraud in recent months and has discovered various warning signs. We believe there is a greater risk that harmful calls may become a more prevalent problem in the nearest future. Given that the UK has the highest rate of fraud calls among all of the European nations, it is essential for communication providers (or "CP") to come to an agreement on a workable approach to address this pressing problem. The degree and kind of harm caused by number spoofing are unquestionably becoming out of proportion. Scammers are determined to manipulate people into disclosing personal information, thus it is the CP's and all parties involved responsibility to prevent such actions from occurring and it is essential to educate any vulnerable people who may be impacted or targeted. This has a significant negative effect on CPs' general operation as well as their reputation. Everyone will be impacted, thus it is imperative to find a solution that will be advantageous for all parties concerned.
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 data spoofing.	*Is this response confidential? – No* Despite the fact that the newly implemented standards and industry efforts are anticipated to help minimise fraudulent calls, more has to be done to combat spoofing. Colt supports Ofcom's efforts to minimise nuisance and scam calls, however, the proposal must be feasible for all types of communication providers. B2B wholesale and enterprise customers normally have a significant international operations and therefore, have quite diverse needs in comparison to residential end-users. Consequently the proposals need to bear in mind the standards adopted in other countries to avoid complexity and incompatibility. As discussed within the consultation itself, having a numbered database could be advantageous even without the CLI

	authentication implementation. If the blocking of mobile calls could be achieved through the introduction of a common database where any operator can check whether any subscriber is roaming or not, this would enable communication providers to minimise the amount of spoofed calls leaving their networks. Additionally, enhancing the CLI blocking approach would be beneficial for the industry as a whole. If each CP were held accountable for conducting their own screening, unwanted/spoofed calls would be removed at source rather than reaching the end-users. The duty to maintain a valid and dialable CLI should remain with the originating CP. Having trusted partners as well as a well-developed blocking/due diligence mechanism would be a priority. If the call is coming from an untrustworthy source, the call should be blocked immediately. Of course, blocking carries its own set of advantages and disadvantages; consequently, CPs should have the technological capability to block calls, which would minimise the issue of disparity. There is a necessity to have a standardised approach, to ensure an even playing fields for all communication providers. At the moment, none of the diverse measures put in place in the UK or by other countries have succeeded in addressing the spoofing issue accordingly. Lastly, Colt would like to conclude that pursuing an international partnership/collaboration should be acknowledged and taken into consideration.
Question 5.1: Is the approach to CLI authentication we have outlined feasible and workable?	*Is this response confidential? – No* The proposed STIR/SHAKEN strategy is a good approach for labelling calls, however, such method does not tackle the issue of scam calls in itself. The proposed approach does not directly prevent a fraudster from spoofing a caller ID, however, it does allow upstream points to decide whether or not to trust the particular ID. Ofcom should learn from other countries where STIR/SHAKEN was implemented, e.g. United States or France. The use of this approach in the United States should be carefully scrutinised. The implementation had a limited success and industry is considering alternative methods to address spoofing. The CLI authentication approach has its limitations, meaning that it is still possible for fraudsters to find their way around the proposed solution. It is important to note the fact that the authentication process does not reveal the validity of a call. Colt is strongly in favour of the European approach, therefore, we should follow the French strategy which is currently being implemented. France has certainly taken into consideration all of the challenges observed in the US and has worked on a more effective solution.

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? – No* CLI authentication improves the screening of malicious calls and facilitates the traceback of calls. However, it has a minimal effect on reducing the amount of scam call and other unwanted calls. Therefore, as mentioned in question 4.1, it is critical for Ofcom to allow time for new measures to take effect and to carefully analyse them, as well as to take a systematic approach to reviewing and developing regulatory interventions. In order to evaluate the most suitable approach, it is important to redesign and carefully examine the current rules and regulations. We should not assume that the STIR/SHAKEN approach is necessary without assessing results of current / new interventions. Before opting for a specific, expensive and potentially inadequate solution such as authentication, Ofcom should evaluate the effectiveness of other measures such as its recent Know Your Customer (KYC) guidelines. It should also consider monitoring the effectiveness of carriers acting on complaints from other carriers. Ofcom may have a role in encouraging debate on alternative pricing models (such as charging per call attempt) but it should avoid direct intervention in commercial pricing decisions.
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? – No* *N/A*
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? – No* In order to ensure full compliance, Colt agree that monitoring and enforcement rules are necessary. If CLI authentication administrator finds that a provider is not taking appropriate action to comply with the rules, it should be required to place the provider into a period of enhanced monitoring and supervision. If there is continued non-compliance by the provider, then the CLI authentication administrator can refer the matter to Ofcom for a formal enforcement action. The CLI authentication administrator cannot impose sanctions on UK members, but may be able to suspend or expel non-UK providers (who join voluntarily) in the event of serious non-compliance to protect the integrity of the CLI authentication regime. Colt has further evaluated its view on the notion of attestation in question 6.2.
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? – No* Colt agrees that the CLI authentication could make call tracing easier. The carrier is attesting to a certain level of confidence that the caller ID has not been spoofed. Signing the call defines the trust and can guarantee that the number used can be effectively transited or terminated. Considering the fact that this approach

	is applied correctly, an unsigned call should be automatically prevented and blocked. We believe that the French approach is certainly efficient, and that attestation should be made compulsory. In France CPs have established and become a member of the CLI authentication administrator. The membership rules govern the implementation and operation of CLI authentication, address how the attestation regime works, set out how the administrator would monitor compliance, and establish which measures could be taken against providers that fail to comply. The administrator plays a central role in monitoring its rules, identifying issues, and taking action to ensure the effectiveness of CLI authentication by its members. Providers should report any instances of non-compliance to the administrator, which would collate this information and pass it to Ofcom for possible enforcement action. As such, on top of the administrator, authentication can only be efficient if a strong enforcement framework and authority is defined/involved. As described above, this particular approach would be beneficial for labelling calls but not necessarily for tackling the issue of spoofing in itself.
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? – No* Implementing CLI authentication is time consuming and expensive. Every minor element must be carefully considered. It is important to thoroughly assess Ofcom's CLI blocking regulations, which have just recently been revised. Colt believes that the industry as a whole, should not assume that the CLI authentication / STIR/SHAKEN approach is necessary prior to assessing the results of all the current and new interventions. Colt is in the process of implementing the STIR/SHAKEN approach in France, and we can attest that the delivery of such an approach is time consuming (several years) and expensive and requires consensus across and collaboration across the industry. Since the implementation process in France has already been underway for three years and is not yet finalised, a longer timeframe should be taken into account to ensure smooth implementation in the UK. It's critical for Ofcom to recognise that this is a brand-new strategy that needs to be established and that numerous additional consultations will be necessary to evaluate all potential difficulties.
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? – No* The assumption is that CLI authentication would be present only on IP networks as the vast majority of legacy networks in the UK are expected to have been decommissioned and replaced by IP networks by the end of 2025. The regulatory scheme would require a further consultation on the detailed regulatory requirements before a final statement confirming the decision, providing telecoms providers with a reasonable period to implement CLI authentication. All providers would need sufficient

	time to establish the administrator, trial operational processes, procure and develop technical systems, which would be broadly consistent with the migration to IP services. To ensure technology neutrality, IP migration should be completed first. Providers should be able to create their own authentication service or outsource it to a third party. The authentication service would also require processes and tools to manage the secure creation and storage of certificate information. Terminating providers would require a verification service to check attestation passports and authenticate the CLI authentication. In relation to the governance framework the proposed CLI authentication administrator should be established by telecoms providers. We agree that the administrator should decide on policies relating to its functions and put in place the systems to carry out the technical functions for CLI authentication. However, those should be considered with the wider industry in order to ensure compliance from all CPs. Providers would need to register with the administrator and interfaces would need to be set up to enable the creation of certifications by originating providers and the verification of attestation passports by terminating 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? – No* The requirements, design, and architecture of the database would need to be decided, and it would need to be funded and administered. The telecoms industry should ideally agree on the most efficient finance and administrative approach. While a common numbering database might not be an essential element of the CLI authentication process, many countries have such databases because of the wider benefits they offer. Such strategy has numerous advantages, but it would require a rigorous re-evaluation of the entire timeframe in order to consider the prospect of a common number database inside the UK. For instance, France has decided against implementing such system, because the lengthy process made it impractical to do so within the allotted time. As a result, the deadline would ideally need to be greater than three years in order to ensure a smooth delivery. It is also important to understand that the majority of CPs will experience certain technical limitations. A live database with roaming and porting information would be incredibly valuable, however, it is critical to underline the risks involved with its implementation Finally, if Ofcom moves forward with its proposed numbers database, this might be a highly overengineered strategy and an

	expensive solution that would make it simple for scammers to adapt and work around the new strategy.
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? – No The overall CLI authentication solution undoubtedly has several advantages, which would be beneficial for the entire industry. However, the STIR/SHAKEN approach must be refined in order to achieve its objectives. Ofcom's primary objective is to limit and reduce the harm caused by scam and nuisance calls; nonetheless, as mentioned above, such an approach is unlikely to reduce the number of spoofed calls. Additionally, Colt is unsure to what extent Ofcom will be able to limit the costs incurred by legitimate businesses. The CLI authentication approach is known to be highly expensive. Finally, the proposed domestic measures appear much more watertight than the proposed approach to incoming international calls, hence there is distinct risk of migration by scammers to overseas platforms if the UK side is successfully closed down. Therefore, the spoofing issue we are currently facing with will not disappear.

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