# 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*<br><br>Hiya agrees with Ofcom's assessment of the risk and damage associated with call spoofing. We only wish to emphasize that call spoofing is only a tactic used to create some of these damaging calls. Even in markets where CLI authentication solutions have been deployed, unwanted and illegal call activity has adapted to other techniques (e.g., short-term number leasing) to continue their practice. |
| **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*<br><br>We agree that more can be done in the UK to reduce scam calls and tackle number spoofing. As mentioned in sections 4.51, 4.52 & 4.53, the US, Canada and France have all introduced a CLI authentication mechanism to try to protect users from fraud. However, as observed in the US where the STIR/SHAKEN framework was first instituted, consumer complaint rates for fully verified (not-spoofed) calls continue to be significant. As such, eliminating spoofing, while it holds promise to reduce spam and fraud activity, is not a complete solution. Spam analytics that models call activity, whether associated with spoofing or not, is required in addition to CLI authentication in order to stop spam and fraud calls. In fact, the FCC in the US is considering an order that may require all terminating operators to use spam analytics to fight spam.<br><br>We believe that BT/EE is currently leading the pack among network providers to solve this problem in the UK. To truly shut down scam and nuisance in the UK, all carriers need to employ a network-based spam analytics solution. |

| | |
|---|---|
| | Hiya agrees with Ofcom that a comprehensive and standardized CLI solution to attack the challenge of call spoofing is one piece of a necessary response to the current threat. However, call authentication is an additional data insight that joins the comprehensive suite of insights that comprise "spam analytics". Spam analytics services observe every call to look for patterns that would indicate if the call is spam, including which carrier originated the call, what country it came from, and if its network signature indicates spam risk. By constantly monitoring these patterns, Hiya's system is able to detect spam calls based on shifting tactics instead of relying on phone numbers and historical data.<br><br>We disagree with statement 4.45 that the effectiveness of such a network-level partnership with Hiya is unclear. Hiya is detecting 28% of all calls outside of the address book in the UK to be unwanted, supported by over 3 million complaints received each month from UK citizens. We are able to provide protection and warning on 100% of these calls detected through analytics today. Given the difficulty of a UK-wide network spam analytics system, it will be necessary for each carrier to include spam analytics at their network level to reach the protection that is envisioned. |
| **Question 5.1: Is the approach to CLI authentication we have outlined feasible and workable?** | *Is this response confidential? – N*<br><br>Although Hiya recognizes that the regulatory and industry environment in the UK is unique, there is considerable benefit in evaluating the experience in the US with CLI authentication in the form of the efficacy of STIR/SHAKEN. In the US, the goal of being able to block calls without attestation has proven so far to be unrealistic, and the situation shows no signs of changing in the near future. To reach the goal of blocking unattested calls, the industry must seamlessly and completely implement a complex set of policies and network technologies. So far the US, after 3 years of mandated CLI authentication, is still very far from reaching the tipping point where lack of |

| | |
|---|---|
| | authentication can be used to block calls without causing considerable problems for legitimate callers for whom authentication is out of their control. |
| **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*<br><br>This stated approach to CLI authentication is similar in nature to the US FCC mandate of STIR/SHAKEN more than 3 years ago. The experience in the US demonstrates that fully verified (non-spoofed) calls continue to have a significant complaint rate of both nuisance and fraud calling. Eliminating spoofing is not a complete solution. Spam analytics that employ machine learning across recipient reactions and call trends to detect spam call activity - whether associated with spoofing or not - is required to stop the scourge of spam and fraud calls. It has been proven in the US that STIR/SHAKEN is not enough as all 3 major US mobile carriers have employed an additional form of spam analytics to protect their subscribers from the potential danger associated with merely answering an unlabelled phone call. |
| **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*<br><br>As stated in section 6.2, 100% of CLI authentication is going to be a difficult bar to reach and there will be unattested calls that are legitimate and need to be connected. This will cause loopholes that can be exploited by scammers. Conversely, we are observing that a significant number of calls that are fully attested in the US under the STIR/SHAKEN framework are in fact unwanted. By labeling calls (i.e. 'spam risk, 'fraud risk', etc.) through analytics that leverages CLI authentication as one of many detection signals, Hiya is able to notify recipients about the risk associated with the call - thereby ensuring protection with or without CLI authentication on the call. |
| **Question 6.1: Do you agree with the approach outlined for the monitoring and enforcement of the rules with regard to CLI authentication?** | *Is this response confidential? – N*<br><br>Hiya has no comment. |

| | |
|---|---|
| **Are there any alternative approaches that we should consider?** | |
| **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*<br><br>Hiya agrees that a very important role of CLI authentication is for traceback of calls to their originators or originating networks. This traceback, where accompanied by strong enforcement, is very powerful in identifying scammers and their use of the network. We also believe that CLI signing information, in combination with spam analytics that can use it in pattern matching, is a key tool for machine learned systems to identify risky calls. |
| **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*<br><br>Hiya has no comment. |
| **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*<br><br>Hiya has no comment. |
| **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*<br><br>Hiya has no comment. |
| **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*<br><br>Hiya has no comment. |