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* We agree with the analysis.
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* We agree that more needs to be done to prevent number spoofing – and that, moreover, regulating call authentication is only a foundational step. STIR is not an end in itself, but instead a platform on which a suite of security services can be built. In the absence call authentication, however, other measures are at best partial solutions, and can sometimes do more harm than good. Many unilateral measures do not fare well in environments where spoofing is undetectable. We also believe it is crucial to engage with the enterprises whose customers are often the victims of such scams, as they are among the primary beneficiaries of call authentication. Enabling enterprises to participate in the UK deployment of call authentication would be beneficial.
Question 5.1: Is the approach to CLI authentication we have outlined feasible and workable?	*Is this response confidential? – N* The examples of the United States and Canada prove that a STIR-based approach is feasible and workable, even in countries with a very diverse set of carriers and a mix of IP-based and legacy systems in place. We believe that the approach Ofcom has outlined in feasible. Also see our answer to 5.3 below.
Question 5.2: To what extent could adopting this approach to CLI authentication have a material impact on reducing scams and other	*Is this response confidential? – N*

unwanted calls? If you consider an alternative approach would be better, please outline this and your reasons why.	A STIR-based solution yields a material impact on reducing spoofing, which in turn reduces the ability of fraudsters to safely launch scams. The non-repudiable PASSporT tokens it generates are also a highly defensible piece of evidence when taking enforcement actions. Adopting a non-standard alternative to STIR for caller authentication would be out of step with emerging deployments around the world, including existing deployments in Europe and North America, which would reduce the potential for international interoperability, and moreover lose the benefit of existing implementation of STIR by major telecom vendors. There are of course measures that can be implemented in parallel with STIR, and as a part of pre-STIR implementation, that can have a material impact on reducing spam calls. Some of these are discussed below in 5.3.
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* Certainly, adopting stricter policies for the use of +44 presentation numbers by entities originating calls outside the UK promises a substantial reduction in scam calls. But since many legitimate calls are also originated in that fashion, including by offshore call centres, STIR solutions like delegate certificates offer a way of distinguishing that legitimate traffic from illegitimate traffic. Ultimately, call validation and treatment services that make decisions about how calls are rendered to users rely on many indications, of which STIR PASSporTs would only be one. Building on STIR's assurance, analytics that can detect anomalous or fraudulent behaviour can help stop problem calls before they reach end users, or signal to users that there is a risk associated with the call. We believe that analytics benefits greatly from the sorts of data that STIR deployments innately generate.

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 agree with the outlined approach.
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* The fact that STIR generates a non-repudiable, timestamped token that establishes which operator vouched for a given call means that STIR is essential to traceback. While it is possible to do traceback without such a token, the hop-by-hop transitive trust of legacy networks can often make this process quite complicated, and not always conclusive.
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* Practically speaking, in North America, the mandate for STIR/SHAKEN deployment came into effect around two years after the passing of the 2019 TRACED Act. Given that so many industry vendors have implemented the various components of STIR today, the UK can rely on those existing standards and implementations to expedite deployment. STIR-based solutions are most effective in an all-IP environment, so potential timelines for STIR deployment in the UK seem to be aligned with the schedule for the IP transition. We do believe that if the UK is going to implement a STIR-based direction, it is essential to begin testing as soon as possible.
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 believe it is now well understood how to stand up the necessary governing entities for a STIR system. Experienced marketplace players have implemented the necessary certification authorities and related systems for other nations, so there are existing systems and governance practices that could be reused by the UK.

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* In order to leverage STIR in real-time to detect problematic calls (as opposed to using STIR for post-facto forensics), participants in the system need to know which carrier(s) should be using a given presentation number. So, the existence of some kind of numbering database is essential, and it is ultimately better that it be a communal database. That said, experience in North America shows that analytics providers of various kinds will leverage a host of factors for determining in real-time how a call should be presented to an end user, which may include probabilistic analysis of the historical and recent call patterns associated with particular numbers, as well as deterministic knowledge about number allocation and validity. In short, a common number database is a very useful asset, but it likely will not encompass all of the data that analytics providers would leverage to make decisions about calls. Ultimately, our assessment is that STIR adds value in the absence of a common numbering database, and that a numbering database could be deployed as a later phase.
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 impact assessment. It is also crucial to recognize that STIR can enable new commercial services for both operators and enterprises, including branded call display (per Ofcom's Objective 2), which can mitigate the costs associated with the implementation of STIR.

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