Your response

Question	Your response
Question 3.1: Do you have further views about the implementation of STIR?	The NICC ND 1522 4 V1.1.1 (2018-04) Report supports the long term solution could be that originating customers are able to sign their own CLIs, and the checking of signatures could be done by terminating customers themselves, which is STIR. However, it does acknowledge that this is the long-term solution. The Report states that although an Interim Stage does not provide absolute authentication of all Presentation Numbers used for display, but it may be that this limited level of signing is sufficient to re-establish public confidence in CLI. The hurdle to establish reliable governance on such a large and diverse range of call originators including a scalable trust mechanism is extremely high even as the STIR protocol spec could allow for this approach. Thus the Interim Stage is of critical importance if the UK is to restore confidence in CLI in a reasonable timeframe. Furthermore, the Interim Stage needs to address call originators using the same Presentation Numbers on multiple networks (ND1522 section 5 STIR Concept, bullet 1) given this is customary practice. The Federal Communications Commission (FCC) and the Canadian Radio-television and Telecommunications Commission (CRTC) have been encouraging the telecommunications industry to develop a solution to stop robocalls and spoofed CLI since 2014. The United States and Canada will deploy Signature-based Handling of Asserted information using toKENs (SHAKEN) as industry framework. STIR defines a set of protocol level tools that can be used in Session Initiation Protocol (SIP) for applying digital signatures to the Caller ID or telephone number of the calling party. Typically, IETF standards are not accompanied by governance, management, cost nor operational considerations so the UK will need to consider all of these in the deployment of STIR. SHAKEN, an ATIS standard created jointly by

	ATIS and the SIP Forum, was developed in order to address those gaps in a way that would scale nationwide and foster trust amongst participants. iconectiv supports the implementation of STIR/SHAKEN in the United States and recognizes that it will become one of the important methods for combating illegal spoofing and will aid in the reduction of robocalling.
Question 3.2: Are there any other approaches we should consider for addressing CLI authentication?	The NICC ND 1522 4 V1.1.1 (2018-04) Report provides insight and details regarding the implementation issues should it be decided to adopt STIR technology in UK networks and identifies the remaining limitations in eliminating nuisance calls and acknowledges SHAKEN as an implementation option. Based on response in 3.1, it is suggested that SHAKEN be considered as the preferred approach for CLI authentication. The ATIS specifications have already been published and accepted by the FCC and the CRTC. These specifications provide a Reference Architecture and the necessary specifications for Certificate Management. A testbed had been established and the major vendors and service providers have tested the protocols and core functionality of SHAKEN as well as major service providers conducting interoperability testing. The greatest drawback to STIR/SHAKEN is the dependency on SIP interconnection end to end between originating and terminating networks, and anything in between. With the UK retirement of BT PSTN infrastructure by 2025 and the goal to cross an All IP Network tipping point along the way, this SIP dependency could be only a minimal and short-term hindrance to widespread CLI authentication in the UK.
Question 3.3: Do you agree a common database would be required to support the implementation of STIR?	The NICC ND 1522 4 V1.1.1 (2018-04) Report states that as the CLIs used by originating networks can be subject to number portability, inherently this means that the record of number assignments will need to be at an individual number level, i.e. a Central Database of individual numbers (CDB). It is recognised that this would add considerable cost and complexity to STIR implementation, but without that database, there is no way of assessing that an originating network has the

	rights to sign a given CLI (to phrase this a different way, STIR without a CDB will identify which network originates a call, but not whether the CLI used on that call is one for which it has rights). The NICC ND report section 5 STIR Concept bullet 1 further suggests that there needs to be a delegation path from the end-customer to their chosen originating network operators in order to authorize signing CLI when the originating operators have not been assigned said CLI by the regulatory authority. Combining these two imperatives suggests that a common database is necessary to identity which originating network has the right to sign a given CLI in addition to providing an authoritative mechanism to enable other originating networks to sign the same CLI under the appropriate conditions. Furthermore, a common database would assist with the porting of numbers as well as the evolution to IP as will be discussed later. A short-term approach without a common database requirement could be implemented if the originating service provider was also the service provider who allocated and provisioned the number. That originating service provider would only need to access their own numbering inventory to provide full attestation for that given telephone number. If the originating service provider did not recognize the number, the highest level of attestation would not be provided. It should be noted, that there is a level of trust in the terminating network that the originating network had the authority to sign. This would only be valid for a segment of calls but could be implemented prior to the deployment of a CBD for all calls.
Question 3.4: What are your views on using blockchain technology as the basis for a common numbering database to support CLI authentication? What other solutions do you think should be considered and why?	It is clear that many companies have significant interest in DLT/Blockchain technologies and are trialing Proof of Concepts in order to determine the cost/benefit. Since blockchain is essentially a continuously growing list of records it allows data to be added to the database: altering or deleting previously entered data on earlier blocks is impossible. Blockchain technology is therefore well-suited for recording events,

	managing records, processing transactions, trading assets, and voting. These are all based on a need to ensure recorded events cannot be tampered with causing value to be siphoned off, supply chain components compromised, key decisions unduly influenced, etc. However, assignment of telephone numbers to end-customers does not appear to carry the same weight and may not justify a blockchain architecture. When evaluating the cost/benefit of Blockchain or any other technology, care should be taken to consider the use cases, key vulnerabilities to guard against, and the outcomes desired. In telecommunication, central databases are incredibly widespread. They cover customer identity and billing information, registries of numbers, supply chain management data, configurations of equipment, maintenance and service logs, geospatial locations of equipment, settlement data, and hundreds of other uses. Some are efficient and fault/fraud-tolerant, while others can be expensive or slow for the various participants. Potentially, all could be "touched" by DLT/blockchain, reducing costs or removing friction, as well as new use-cases emerging from its decentralized properties. It should be noted that there is a distinction between public and private blockchains and in the case of national number databases the discussion should be in the context of private blockchain. The core problem that the classic public blockchain aims to solve is achieving and maintaining integrity in a purely distributed, peer-to-peer system comprised of an unknown number of peers with unknown reliability and trustworthiness. A public and permission less blockchain is not suitable as there is no currency incentive, nor should it be an open network where anyone can join, nor is it meant to share the record of a call between two networks with all of the other participant networks. For these reasons, private and permissioned blockchains exist. A private and permissioned blockchain is designed to allow an organization or a consortium of organizations to efficiently exchange information and record transactions.

	They use consensus mechanisms that are less computationally expensive in comparison to the classic proof-of-work, which allows them to enjoy better scalability and performance than public and permission less blockchains. Nonetheless, we should consider that illegal robocalling is a multi-billion dollar industry where adversaries leverage spam and scam calls to commit consumer and telecom fraud on a grand scale. So the perpetrators are highly motivated to make every attempt to participate in the solution as well as compromise the framework. In effect, this is still a hostile environment even in a permissioned private Blockchain. So whether we use Blockchain, a traditional database or some other technological construct, it will be of key importance to ensure there is trust amongst the participants, these participants are thoroughly vetted before their calls receive authenticated CLI and there is a solid governance model to weed the bad actors out. Given the current commercial deployment status of Blockchain implementation, more trials would be prudent prior to finalizing on a technology. For example, GSMA is working on Solid (a set of conventions and tools for building decentralized social applications based on Linked Data principles) and information stored in Personal Online Data store (PODS - A secure repository containing the user's data. Users control application access to their POD(s). Solid is built on a linked data model, which uses the web to create a globally distributed graph. Everything in linked data has a URI, and can be linked with any other thing. Things in linked data are defined by shared vocabularies and data shapes. Vocabularies and shapes provide native interoperability of data even when it is stored in different places.
Question 3.5: What are your views on timeframes?	Since the specifications are already available for STIR/SHAKEN the timeframe for implementation could be in the 18-24 month period. If the governance required to support Presentation Numbers originating on multiple networks requires further consideration, perhaps begin with the traceback elements in STIR/SHAKEN and begin feeding this valuable information to analytics engines as well as

	regulatory stakeholders in order to stop more robocalls both in real-time and by more timely enforcement after the fact. The timeframe for adoption of a national database requires more of a glide path given the utilization of such a database could have multiple purposes including CLI identification, number portability and transition to IP.
Question 4.1: What are your views on the current implementation of number portability in the fixed and mobile sectors?	No response
Question 4.2: What are your views on sharing the functionality of a common numbering database for CLI authentication to also support improvements in UK porting processes?	Yes, the use of a common database could have multiple feature functionality including the use for number portability, CLI authentication, and IP transition.
Question 4.3: We are currently supporting a blockchain pilot. Do you have any views on using this technology for port transactions and a routing database? Are there other alternatives that should be considered?	Per our response to 3.4, the cost/benefit analysis for the agreed use cases and outcomes desired are key and we look forward to hearing the results of that analysis from the Blockchain pilot. The suitability of this vehicle for port transactions and IP routing is not so much a question of technical feasibility but rather of cost and complexity and their impact to scalable operations and governance.
Question 4.4: What are your views on implementation timeframes and the importance of a common database solution being available to support the migration of telephony services to IP?	Having a common database enables the transition to IP in a more efficient and effective manner. There will be one network operator authorized to write the database for a given CLI in any one instance, with billions of relying party (other network operators) transactions reading the database.
Question 5.1: What are your views on the potential for a common database solution to also provide shared functionality to support number management?	Technically, Number Management could be an integral part of a common database. Providers could utilize the common database for number assignments In addition to the other transaction types discussed in this inquiry.
Question 5.2: What do you see as the benefits or disbenefits of changes to number management post PSTN retirement?	It is iconectiv's opinion that numbers will be allocated in blocks to large providers even in a post-PSTN environment. This enables those Service Providers some flexibility in Number

	Management and inventory. The blocks do not need to be as large as they are today and could be managed according to size of customer base, need, etc.
Question 6.1: Do you agree, in principle, with the need to develop and adopt a common numbering database? If not, why not?	Yes, iconectiv agrees in the development and adoption of a common number database. The rational has been provided in preceding sections
Question 6.2: If you do not agree with the need to develop and adopt a common numbering database, do you have any suggestions on how the issues we have set out in this consultation could be addressed?	
Question 6.3: Do you agree that in the first instance industry should lead the implementation of a common numbering database, with Ofcom providing support to convene and coordinate key activities? If not, what are your views on how implementation should be taken forward?	Yes, iconectiv supports that the industry should lead in the implementation with Ofcom providing the necessary support.