Your response

Question	Your response
Question 1: Do you agree with our proposed modification of General Condition C6.6? If not, please give reasons.	*Is this response confidential? – No.* Transaction Network Services, Inc. ("TNS") supports the proposed modification of General Condition C6.6 to the extent it relates to invalid and non-dialable numbers. TNS respectfully

	submits that the proposal requires further modification with regards to numbers that do not uniquely identify the caller. Determination of whether a number identifies the caller would benefit from the deployment of call analytics in telecoms carrier networks and the deployment of a call authentication system similar to the STIR/SHAKEN framework deployed in the United States. *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859 (2020). https://www.fcc.gov/document/fcc-adopts-new-rules-combat-spoofed-robocalls-0 While blocking of calls that fail to include valid CLI can play a role, TNS has found that blocking alone has a limited effect because scam callers that currently pass invalid CLI can easily shift tactics to other methods to complete their calls. In order to have a meaningful impact on the volume of illegal calls, service providers should implement call analytics solutions in their networks and the industry needs to deploy call authentication on a widespread basis. *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876 (2019). https://www.fcc.gov/document/fcc-affirms-robocall-blocking-default-protect-consumers-0 Please see the explanation below.
Explanation: TNS is an industry leading call analytics solution that uses cross-carrier, real-time call events combined with crowd-sourced data to create accurate and comprehensive reputation profiles to differentiate legitimate users of telecommunications services from abusive, fraudulent and unlawful users. TNS' Call Guardian service utilizes information from over 1 billion signaling transactions per day traversing the TNS signaling network and IP call routing databases to differentiate legitimate uses of communications services from illegal and unwanted calls. TNS' Call Guardian service is a robocall detection solution implemented in the United States by four of the six largest wireless carriers, by major cable VoIP providers and over a hundred rural wireline and wireless carriers. To date, over 105 million subscribers in the United States receive call blocking and call labeling services through TNS' voice service provider customers. In response to rulings by the U.S. regulator, TNS scores calls with invalid, malformed and "Do Not Originate" numbers as likely illegal calls. Most of TNS' carrier partners choose to block these calls from completion to their customers. As a result, it is the norm among TNS customers that calls with invalid or non-dialable numbers are blocked. These calls represent only a small portion of the total call volume, however. TNS estimates that calls with invalid or non-dialable numbers are between 2 percent and 5 percent of all calls it processes with Call Guardian. One reason for this is	

that TNS has found that callers that previously would transmit calls with invalid numbers changed tactics and would transmit calls either with valid numbers closely associated with the called party ("neighbor spoofing" of calls), with numbers of well-known commercial providers or with toll free numbers. According to TNS' most recent Robocall Report, toll free calls were the second-largest source of unwanted calls in 2021. Many of those calls used spoofed numbers. Therefore, while TNS supports blocking of calls that contain invalid or non-dialable CLI data, this measure will not have a significant impact on consumer experiences because scam call originators are likely to shift tactics upon implementation of such a rule. *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706 (2017). https://www.fcc.gov/document/fcc-adopts-rules-help-block-illegal-robocalls-0

With respect to calls that do not uniquely identify the caller, it is not easy for downstream telecoms providers to know this information. Determination of whether a number identifies the caller would benefit from the deployment of call analytics in telecoms carrier networks and the deployment of a call authentication system similar to the STIR/SHAKEN framework deployed in the United States. TNS supports the agency's plans to explore the implementation of technical standards for CLI authentication in the near future. This step – equivalent to the introduction of STIR/SHAKEN in the United States – will assist telecoms service providers and analytics providers in identifying scam calls and tracking their tactics more closely. *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859 (2020).

TNS also encourages the agency to take steps to increase the use of call analytics in the UK. In the United States, the Federal Communications Commission has implemented a safe harbor protection from liability for blocking if service providers rely upon "reasonable analytics" to identify and block calls, subject to a procedure for legitimate callers to seek redress from service providers for erroneous blocking. Such a program in the UK will enable telecoms service providers to better protect their customers by dynamically identifying and blocking scam and other unwanted calls. TNS recommends that the agency explore the use of analytics to identify and protect against scam calls. *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876 (2019).

Question 2: Do you agree with our proposal to bring this modification into force six months after the publication of our statement (which is planned for Autumn 2022)? If not, please pro-vide reasons why a different date would be appropriate.	*Is this response confidential? – No* TNS does not take a position on when such a modification should take effect. TNS encourages the deployment of call analytics as soon as practicable and the development of a call authentication framework promptly.
Explanation: n/a	
Question 3: Do you agree with the proposed changes to the CLI guidance? Please provide reasons for your response. Please set out your comments on each of the proposed changes separately.	*Is this response confidential? – No* TNS is not a telecoms service provider and does not take a position on whether the proposed changes to CLI guidance should be implemented. As explained below, some of the proposals may have limited impact on scam calls, while the use of analytics can improve the ability of telecoms service providers to comply with other CLI guidance.

Explanation: As noted, proposals to block calls that do not contain a 10 or 11 digit originating number (4.8) or that are on the DNO list (4.12) are not likely to have a significant impact on unwanted call volumes, as scam callers likely will shift to new tactics to avoid the prohibition.

With respect to the guidance in 4.13 that providers may use "other sources of information" to identify and block spoofed calls, such blocking and, in other instances labelling, is only possible with the use of call analytics such as those provided by TNS. Ofcom can improve the ability of service providers to identify spoofed numbers through policies that permit and promote service providers to use analytics services. As noted in response to question 1, in the United States, the regulator adopted a safe harbor from liability for providers that use reasonable call analytics to identify and block unwanted calls. TNS respectfully submits that Ofcom should evaluate whether similar policies are appropriate in the UK. *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876 (2019).

Finally, TNS similarly notes that call analytics can play a role in the ability of telecoms service providers to block calls with invalid CLI that originate abroad (4.18-4.30). TNS respectfully suggests that Ofcom consider acknowledging the role of call analytics in this portion of its guidance.

Question 4: Do you have any comments on the use of 084 and 087 non-geographic numbers as Presentation Numbers and/or on the impact if the use of 084 and 087 numbers as Presentation Numbers was prohibited in the CLI guidance? Are you aware of any examples of the use of 084 or 087 numbers as Presentation Numbers?	*Is this response confidential? – No* TNS does not take a position regarding the use of 084 or 087 numbers. TNS notes, however, that, in the United States, spoofing of non-geographic numbers, especially toll free numbers (800, 888, etc.) is a problem. Many bad actors migrated to spoofing of toll free numbers after invalid numbers were blocked.
Explanation: n/a	