Non Confidential

Calling Line Identification (CLI) authentication: a potential approach to detecting and blocking spoofed numbers

Twilio's Response to the Ofcom consultation initiated on 28 April 2023

23 June 2023

1. About Twilio

1.1 Twilio Ireland Limited is a provider of electronic communications services in the UK, and has been granted rights over UK numbering resources by Ofcom.

1.2 As a leading global Communications Platform as a Service (CPaaS) provider, Twilio provides services to more than 285,000 enterprises globally and powers more than 1 trillion interactions between them and their customers every year.

1.3 Twilio's software allows customers to communicate with their customers over voice, SMS, messaging, or email thanks to the communications feature that companies have added into applications across a range of industries, from financial services and retail to healthcare and non-profits.

1.4 Twilio serves a number of global customers as well as Government organizations. Many of Twilio's customers are also small and medium-sized enterprises. Twilio's non-profit arm, Twilio.org, supports charitable organizations to deliver their communications needs, such as the Norwegian Refugee Council, a global NGO supporting refugees worldwide. Twilio is also a technology partner and supporter of the United Nation's Vaccine Alliance GAVI.

2. Introduction and key points

2.1 Twilio Ireland Limited (hereafter 'Twilio') welcomes Ofcom's consultation entitled *"Calling Line Identification (CLI) authentication: a potential approach to detecting and blocking spoofed numbers"*, published on 28 April 2023.

2.2 Twilio takes good note of the fact that Ofcom is providing its initial thinking about how CLI authentication might work in the UK and the extent to which the actions that providers are already taking are likely to address the problem of number spoofing. Twillio also notes the fact that Ofcom is not making any proposals for specific regulatory interventions at this stage.

2.3 Twilio welcomes Ofcom examining the merits of introducing CLI authentication in the UK. Based on its experience with implementation of STIR/SHAKEN in the United States and Canada, and with the preparation of the introduction of CLI authentication in France, Twilio provides what it hopes are relevant insights for Ofcom and for industry in the UK.

2.4 Twilio considers that CLI authentication is potentially part of a set of solutions to address harmful use of numbers, but that CLI authentication is not a comprehensive solution in its own right. In Twilio's view, the most important capability to introduce to deal with harmful activity is to rapidly and reliably determine, based on a traceback, whether a harmful actor is using a number, and to take action against harmful use all the while ensuring that legitimate use is not unduly impeded. Indeed, Twilio's experience shows that the ability to rapidly and reliably perform a traceback to the entity that is in reality originating a call/text is crucial in effectively combating harmful activity, regardless of whether the call/text originates from an entity that uses a spoofed number, or from an entity that has legitimately been given a number in use. This is the case because harmful activity, including automated calling/text, can and does occur not only by entities spoofing numbers, but also by entities that are given numbers in use on a bona fide basis. Ensuring that legitimate use is not unduly impeded, and rapid redress where legitimate use is impeded, is a necessary feature of any envisaged action, be it industry agreed, regulatory, or legislative in nature.

2.5 If CLI authentication were pursued in the UK with a view to detecting and blocking spoofed numbers, which Twilio welcomes with provisions detailed in this response to Ofcom's consultation, particular attention would be needed to the following points:

(a) Ofcom and industry would be well-advised to adopt already existing technical standards to the greatest extent possible, i.e., minimize UK specificity. Not doing so would unnecessarily raise costs for all involved.

That being stated, Twilio's practical experience in the United States is that while STIR/SHAKEN has been deployed as a call authentication mechanism, it does not replace the need for a system enabling the reporting of misuse as well as rapid and reliable traceback to the call originator. STIR/SHAKEN is a mechanism to help enable that, but is not the only mechanism that may be appropriate to achieve this goal. Bona fide Communications Providers are themselves the victims of sophisticated entities intent on misusing telecommunications services, and these entities constantly adapt their practices. A focus on rapid and reliable traceback, to the entity that is in reality originating a

call/text, is key to stemming misuse of telecommunications services, see also point 2.4 above.

(b) UK-wide implementation of IP-interconnection would, in terms of effectiveness, and in cost-benefit terms, be a prerequisite for introducing CLI Authentication.

Whilst some are pursuing solutions to also authenticate circuit-switched calls, the case for supporting a technology that is being phased-out would be very hard to make.

(c) A common number database is not a prerequisite for implementing STIR/(SHAKEN) as a CLI authentication mechanism, as Ofcom itself recognises.

(d) Governance arrangements are at least as important as technical standards and processes and their implementation. It would be of particular importance to ensure that:

(i) All willing Communications Providers have the right to be involved, on equal terms, in defining both the technical aspects and the governance structure of CLI authentication to ensure that terms are not de-facto dictated by the largest Communications Providers. Ofcom would have to be actively present in discussions, with decision-making powers, to ensure that both technical and governance arrangements are defined in a manner which does not negatively affect end-user interests and competition, and/or hamper innovation.

(ii) A single certificate authority (the CLI Authentication Administrator) would be instituted, as Ofcom appears to be suggesting (paragraph 5.25), as well as an unequivocal boundary between the CLI Authentication Administrator function and any Communications Providers, not only in legal terms but also in practical terms. This is necessary to ensure that no undue preference or undue discrimination of Communications Providers occur.[1]

[1] Twilio notes that there are parallel similarities in the approach where for instance number porting is operated through a centralised database.

(iii) Costs would be apportioned in a manner which respects the differing sizes of Communications Providers in the UK. Agreeing a set of threshold values in terms of UK annual revenues and related financial contributions is likely a good way to approach this, as is promoting that the CLI Authentication Administrator and its suppliers would work based on a Software-as-a-Service model.

(iv) The risk of false positives should explicitly be acknowledged and addressed in any formal regulatory measure, as well as in the technical and governance arrangements that would be applied. Therefore, prior to any blocking being implemented, an agreed structured and efficient process should be discussed for each case on a multi-lateral basis between Communications Providers. In addition, where blocking proves to be unjustified or accidentally impedes a legitimate use case, it should be possible for blocking to be undone immediately, and for more effective arrangements to be pursued, in particular going after the entity conducting harmful activity (harmful use may involve numbers that are also used for legitimate purposes, and may well go through multiple Communications Providers) rather than to block number ranges or even the traffic of a given Communications Provider.

2.6 Additional points from the Communications Provider perspective include the following:

(a) Whilst harmful use of telecommunications is an unfortunate reality and should be actively combatted, legitimate innovative use cases of numbers, including Communications Platform as a Service – CPaaS – exist and are growing. CPaaS use cases are appreciated by businesses, government, and end-users (see also Section 2 below). Introducing CLI authentication and/or other measures, be they industry agreed, regulatory in nature, or even legislative in nature, should not result in hampering innovation or restricting competition on telecommunications markets. In addition, conflicts with the Communications Act 2003 should be excluded, in particular as regards the provisions ensuring end-to-end connectivity.

(b) Placing the totality of responsibility for combating harmful activity on Communications Providers is neither appropriate nor realistic. harmful actors are sophisticated and constantly adapt their practices. A CLI authentication system is likely part of the solution but does not replace law enforcement in cases of criminal activity. Ultimately, criminal activity is a matter of law enforcement.

(c) A centrally administered reporting platform and hotline, enabling members of the public, as well as all companies and administrations to report alleged fraud using numbers, alphanumeric SMS, e-mail and in other forms of communication, is likely to be crucial. This would enable reporting, and relevant industry participants to rapidly cross-analyse cases and take appropriate action where and when justified, including reporting cases to law enforcement.

2.7 Twilio looks forward to studying the elements that will be provided by other respondents to this consultation, and to Ofcom's full impact assessment.

3. Brief comments on Chapter 2: Ofcom's introduction

3.1 Twilio welcomes Ofcom's introduction, including in particular paragraph 2.10, describing the Policy Objectives, which will frame Ofcom's planned impact assessment. Twilio explicitly agrees with each of these Policy Objectives. Indeed, it has been, and remains, justified for Ofcom to take action aimed at reducing harm caused by scam, nuisance and other harmful calls/texts in the UK. At the same time, it is justified for Ofcom to support legitimate and innovative use cases which are beneficial for end-users, and for competition. Twilio therefore urges Ofcom to stand firm on each of its Policy Objectives, and, in any follow-up work, to avoid contributing (explicitly or inadvertently) to situations in which legitimate calls/texts, legitimate users, and legitimate Communications Providers would face undue blocking.

3.2 In addition there is a need to explicitly and formally acknowledge, in any formal regulatory measure to be adopted by Ofcom as well as in the technical and governance arrangements that would consequently be applied, the risk of false-positives and the need to have an agreed structured and efficient process to deal with false-positives. Each case should be discussed on a multi-lateral basis between Communications Providers with a Service Level

Agreement (SLA) that applies to redress for legitimate calls. This point stands, whichever future steps are taken, including possibly proceeding to the introduction of CLI authentication or further blocking measures, etc. Please also refer to our key points, including in particular paragraph 2.5 (d) (iv) above.

3.3 Where Ofcom's duties and powers are addressed (paragraphs 2.6-2.9) it would be valuable if Ofcom also listed the sections of the Communications Act 2003 and its own instruments where they address end-to-end connectivity.

4. Brief comments on Chapter 3: The Harm caused by number spoofing, including response to Question 3.1

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.

4.1 Twilio agrees that the UK is facing a considerable amount of scam calls/texts and nuisance calls/texts, which can harm the consumers and organisations directly affected, weakening trust in the telephone service, potentially leading to further harms if this results in legitimate calls going unanswered. There is however also a considerable risk that inappropriate interventions could result in a situation in which legitimate calls/texts are unsuccessful, professionals are unable to join important conference calls (joining calls or be reached by the conference calling platform making an outbound call), other essential outbound calls including alert calls fail, etc. as a result of unjustified blocking.

4.2 Twilio also recognises that spoofing is a serious issue as part of harmful calls, and agrees with Ofcom's analysis of the ways in which spoofing can be used to cause harm. It is important, however, for Ofcom to also acknowledge that:

(a) harmful activity, including automated calling/text, can and does occur not only by entities spoofing numbers, but also by entities that are given numbers in use on a bona fide basis. Communications Providers are also victims of entities conducting harmful activity (which may

involve numbers or number ranges which are also in use for legitimate purposes, and which may well go through multiple Communications Providers, unbeknownst to them).

(b) There are legitimate reasons for changing the number displayed to recipients of calls/texts, as Ofcom recognises.

4.3 With regard to (a) above, Twilio's experience shows that the ability to rapidly and reliably perform a traceback to the entity that is in reality originating a call/text is crucial in effectively combating harmful activity, regardless of whether the call/text originates from an entity that uses a spoofed number. Ensuring that legitimate use is not unduly impeded, and rapid redress where legitimate use is impeded, is a necessary feature of any action to envisage, be it industry agreed, regulatory, or legislative in nature.

4.4 With regard to (b) above, Twilio wishes to highlight a set of tangible legitimate use cases, over and above the high-level description provided by Ofcom in paragraphs 3.8-3.13.

The international NGO Child Helpline, for instance, has built a tailored helpline solution for Child Helpline International through Twilio's cloud-based contact center "Twilio Flex". The platform brings interactive voice and text responses online, allowing counsellors the option to hold multiple conversations over phone, social, or text. This upgrade lets counsellors more efficiently manage the queue without sacrificing care quality.

During the COVID-19 pandemic, call volume to child helplines went up by 50 percent, but shelter-in-place restrictions dramatically limited how many staff and volunteer counsellors could respond to the urgent and life changing cases the helplines received. With Twilio Flex, counsellors only need an internet connection and a computer to log onto the platform and begin changing lives. This flexibility is critical in enabling helplines run at full staff and provide a consistent community experience. Through Twilio Flex, the platform will help child helplines soon reach 100 million children annually, helping counsellors address the worst cases of mental and physical child abuse and a range of micro crises such as ending persistent school absenteeism and child marriages.

Similarly, in order to protect the privacy of hospital doctors, services powered by Twilio enable doctors to make calls from their private office or mobile phone but presenting their number at the hospital when calling a hospital patient. This separates the doctor's personal number from the hospital practice but enables the doctor to make after hours calls in urgent cases. The patient can call back to the presented number and will reach the hospital and/or receive information about how their case can be further processed. The same and related features can also be used to remind patients of medicines they need to take, pharmacy appointments, etc. which should not trigger calls/texts back to individual medical professionals which may not be available at the time of the return call/text.

Also, many schools use both phone calls and text messages to notify parents in case of emergency or non-emergency situations or events relating to their children. Staff or teachers will typically wish to provide the school's number, rather than their individual office number or mobile phone number, including to enable parents to contact the school when the person who made the outgoing call/text is absent or otherwise occupied (e.g. teaching a class). The reverse scenario can also occur, in which the school number is used, but inbound calls/texts can be answered from home or on the move by a designated member of staff or by a teacher.

Ride sharing and food delivery platforms also constitute relevant examples, where a communication by call/text can be relevant to initiate and conclude a transaction, but neither the driver/delivery person, nor the customer, wants to expose themselves to receiving unwanted calls or texts from one-another after the transaction has been terminated.

For other relevant references, see Twilio Healthcare solutions, Twilio Nonprofit solutions, and references from Twilio's nonprofit support Twilio.org

5. Brief comments on Chapter 4: Regulatory and market context

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.

5.1 Twilio is aware of Ofcom's work since 2015 to reduce the harm to consumers from nuisance calls, including initiatives such as the Good Practice Guide, the Do Not Originate (DNO) list, the 2021 NICC industry guidance and its application, and the blocking measures addressing spoofed numbers, introduced in 2022. Twilio agrees that this body of work has helped to reduce spam calls/texts, and that it has been successful in putting an end to specific major scams. Twilio agrees with Ofcom that more needs to be done, given the persistently high number of scam calls/texts in the UK.

5.2 Twilio is aware of the UK Home Office's initiatives to deal with fraud, including the Telecoms Fraud Sector Charter, and a new broader Fraud Action Plan presented for consultation this Summer, including suggested legislation. Twilio's preference is that further action by the UK authorities relating to the telecommunications industry would be concentrated entirely under Ofcom's purview, to ensure that there is a single clear interlocutor for the telecommunications industry on these matters going forward.

5.3 As regards measures taken by individual industry participants (paragraph 4.34 and following), Ofcom reports that Communications Providers are implementing initiatives to *"(...) meet (and in some cases exceed) the forthcoming changes to regulatory requirements"*.

5.4 As Ofcom itself notes, there are some imperfections which affect the current rules and industry measures in the UK, resulting in continued problems with scam calls. Twilio wishes to draw attention to other imperfections, which result in currently applicable rules/guidance not always functioning as expected. In particular where Communications Providers "exceed" the existing or forthcoming regulatory requirements, there is a real concern that calls, and calls originating from contiguous series of numbers, are excessively blocked, negatively affecting legitimate use cases, causing recurring work for Communications Providers to unblock their legitimate users' traffic using the same or adjacent numbering ranges, etc., e.g. raising costs for terminating legitimate traffic. Very specifically, there is a concern that some providers' blocklists and call screening software (approaches which Ofcom welcomes, e.g. at paragraphs 4.45 and 4.46) proceed directly to blocking without appropriate consultation with other Communications Providers and the impacts on them. Ofcom acknowledges (paragraph 4.60) that there is little independent oversight of the accuracy of crowd-sourced information, which

could lead to erroneous/malicious marking of calls as potentially being scams. Twilio wishes to add that where unjustified blocking or warnings occur at the terminating end, it takes time for the affected Communications Providers to be made aware that their numbers have been flagged or added to blocklists (or only become aware when their customers complain about their legitimate communications failing). Unjustified blocking or warnings can result from the implementation of crowd-sourced systems but can also result from the implementation of blocklists and other systems deployed by Communications Providers. It also takes time and sometimes fraught discussions to correct errors, including to blocklists. This has substantial negative impact on legitimate users (who often are legitimate UK business users and global businesses, whose communications are unpredictably impeded) and on the Communications Providers that support these users' legitimate communications. Twilio asks Ofcom to also take these elements into account when reporting back on this consultation and when considering next steps. A firmly agreed set of regulations and industry-wide set of governance arrangements and technical processes is needed to ensure that practices employed by Communications Providers, however well intended to protect their customers, do not negatively affect other Communications Providers' users, the forwarding of legal calls and competition and/or hamper innovation.

5.5 With regard to international experience (discussed by Ofcom in paragraphs 4.47 to 4.57), Twilio wishes to highlight that it was deeply involved in the design and implementation of STIR/SHAKEN in the United States. Whilst STIR/SHAKEN has produced material improvements so far in the United States, it has not quite performed as well as expected in some areas. As an example, extensions to STIR/SHAKEN, like the DIV passport, are required to have call authentication work with forwarded calls and that has yet to be supported widely. Additionally, with exemptions for calls not being forwarded using IP-technologies, not all traffic is being authenticated leading to more complicated tracebacks. STIR/SHAKEN does not replace the need for a system enabling the reporting of misuse as well as rapid and reliable traceback to the call originator. As mentioned before, STIR/SHAKEN is a mechanism to help enable that, but is not the only mechanism that may be appropriate to achieve this goal. Bona fide Communications Providers are themselves the victims of sophisticated entities intent on misusing telecommunications services, and these entities may use services

paid for (rather than relying on spoofing third parties' numbers) and constantly adapt their practices in ways that are not easy for Communications Providers to identify. As a consequence, the US Federal Communications Commission (FCC) is now placing additional emphasis on the identification of customers and on users/victims reporting harmful activities and call analytics, which can lead to additional improper blocking or mislabeling of legitimate calls. Given the recurring problems with false-positives affecting legitimate users, interest in the US is also growing for pursuing other technology options (including analytics and artificial intelligence) to deal both with the identification of harmful users and to ensure that false-positives do not interrupt critical business processes of legitimate users.

5.6 In line with Ofcom's suggestions on the potential role of CLI authentication, and given the elements outlined by Twilio in this response, Twilio agrees with Ofcom that, over the medium term, there may be a need for more comprehensive processes than those in place today in the UK and those being brought into full effect shortly in the UK. Twilio considers that CLI authentication is potentially part of a set of solutions to address harmful use of numbers, but that CLI authentication is not a comprehensive solution in its own right. This is in contrast to Ofcom's statement in paragraph 4.62 that *"CLI authentication could provide a more comprehensive solution"*. Ofcom recognises (paragraph 4.68) that *"(...) the time is right to consider, in principle, the introduction of CLI authentication, taking advantage of maturing standards, system availability and implementation learnings and experiences that now exist"*. In Twilio's view, the learnings from the experience include the fact that the most important capability to introduce is the ability, based on a traceback, to rapidly and reliably determine whether a harmful actor is using a number, and to take action against harmful use, all the while ensuring that legitimate use is not unduly impeded.

6. Brief comments on Chapter 5: Ofcom's view on how CLI authentication could work

6.1 Twilio notes that Ofcom's introduction (in particular paragraph 5.5) explicitly makes reference primarily to: *"The methods (...) based on STIR standards, which have already been implemented in the US and Canada, and to a lesser extent, the associated SHAKEN framework (...)"*. Twilio is pleased to note that Ofcom identifies the distinction between STIR and SHAKEN. A focus on implementing STIR, in a way that minimises UK discrepancy from international practice is definitely relevant.

6.2 Twilio considers that Ofcom is right (paragraph 5.13) in considering the relevance of both intra-UK calling and international calls to UK customers. Given the UK's role as a global centre for business in general, and finance, media, and service industries in particular, ensuring that business can be conducted from the UK globally is absolutely essential. Correspondingly this would indicate that the UK is genuinely open for business, including for international partners. Therefore, it is necessary to ensure that the origination of legitimate calls to UK numbers (notably, but not exclusively, those from UK public administrations and businesses), are not subject to unpredictable, unexpected, and unjustified blocking.

6.3 Where Ofcom posits that blocking of calls that have not been successfully authenticated would be the optimal outcome (paragraph 5.18), and that under a regulatory scheme for the implementation of CLI authentication, blocking would be underpinned by a regulatory measure, such as a modified General Condition or updated Guidance to the existing General Conditions (paragraph 5.20), Twilio respectfully asks Ofcom to consider a more nuanced approach.

In Twilio's view, the risk of false positives should explicitly be acknowledged and addressed in any formal regulatory measure, as well as in the technical and governance arrangements that would be applied. Therefore, prior to blocking being implemented, there would have to be an agreed structured and efficient process to discuss each case on a multi-lateral basis between Communications Providers.

In addition, where blocking proves to be unjustified or would accidentally impede a legitimate use case, it would have to be possible for blocking to be undone immediately, and for more effective arrangements to be pursued, in particular going after the entity conducting harmful activity (harmful use may involve numbers that are also used for legitimate purposes, and may well go through multiple Communications Providers, unbeknownst to them) rather than to block number ranges or even the traffic of a given Communications Provider.

6.4 As regards the system envisaged by Ofcom, with digitally signed authentication credentials associated with each outbound call during call setups, Twilio agrees that a trusted third party would be essential – the CLI Authentication Administrator. Twilio explicitly supports the notions (implicit in particular in paragraphs 5.22-5.25 of Ofcom's consultation document) that:

(i) there would be a single such CLI Authentication Administrator in the UK, and (ii) that this single CLI Authentication Administrator would be a body of which all UK providers would be members, and operating in a regulatory scheme subject to the approval of Ofcom.

6.4 Twilio additionally suggests that Ofcom, if it would decide to proceed to introducing such a CLI authentication system, would also commit to be actively present in discussions relating to the establishment and governance of the Body and its governance rules, with Ofcom decision-making powers, to ensure that both technical and governance rules are defined in a manner which does not negatively affect end-user interests, competition or hamper innovation.

6.5 In addition, Twilio would expect that Ofcom would formally determine an unequivocal boundary between the CLI Authentication Administrator function and any Communications Providers, not only in legal terms but also in practical terms. This is necessary to ensure that no undue preference or undue discrimination of (the largest) Communications Providers would occur.

6.6 As regards the potential use of a common numbering database in the UK (paragraph 5.32 and following), Twilio is very clear in stating that this is not essential for establishing an effective STIR/SHAKEN regime or another or improved CLI authentication system. That being stated, Twilio recognises that a central national common reference database may have merits. A centralised common reference database system has been implemented in nearly all EU Member States, initially focused on national use for number portability purposes. Such systems have, in many EU Member states been successful not only in enabling number portability (effectively resulting in porting within one working day without onward routing and without related additional transit fees which are still prevalent in the UK) but also in performing additional agreed relevant tasks, relating to emergency communications, directory services, and national security matters etc. Twilio considers that, in terms of the effectiveness of meeting the applicable regulatory requirements, centralising matters, notably relying on centralised reference databases may have merits. Clearly, in case Ofcom would pursue a centralised database system, possible implementation and all the modalities thereof would have to be subject to detailed discussions with industry prior to any decision-making. A

decisive role for Ofcom, the independent regulatory authority, would be essential in determining, and if necessary, arbitrating on key governance issues.

6.7 The potential of a common numbering database is addressed in paragraphs 5.33-5.37 and in Section 7 of Ofcom's consultation document. Ofcom explicitly states that it does not have a strong view on the matter (paragraph 5.35). Twilio's position in this regard is that a common number database (be it for Network Numbers only, or Network and Presentation Numbers) is not a prerequisite for implementing STIR/(SHAKEN) as a CLI authentication mechanism. Clearly, in case Ofcom would pursue a centralised database system, possible implementation and all the modalities thereof would have to be subject to detailed discussions with industry prior to any decision-making. A decisive role for Ofcom, the independent regulatory authority, would be essential in determining, and if necessary, arbitrating on key governance issues.

As indicated in our key points above, Twilio believes that the most important capability to introduce to deal with harmful activity is in fact to rapidly and reliably determine, based on a traceback, whether a harmful actor is using a number and to take action against harmful use all the while ensuring that legitimate use is not unduly impeded.

6.8 Calls entering the UK from abroad are addressed in paragraphs 5.38-5.48 of Ofcom's consultation document. In November 2022, Ofcom set out legitimate use cases for calls with UK CLI as a Network Number, including in particular the case where the traffic originated from UK customers hosted on overseas nodes or cloud services (including call centres making calls legitimately on behalf of UK businesses). Twilio welcomes the recognition by Ofcom of the importance of cloud-based communications services, and has made efforts, including architectural changes, to maximise the routing calls over pre-agreed identified interconnects. Twilio appeals to Ofcom, when considering next steps, including any further measures that could involve Communications Providers blocking (and being required to block) calls, to be mindful of the fact that cloud-based communications supports many legitimate use cases that are helping businesses and public administrations to be more employee-friendly (e.g. supporting teleworking), more flexible for customers (e.g. enabling organisations to be reached outside office hours), and generally more efficient, including saving money that can better be channelled to fulfilling their core mission. Communications

Platform as a Service (CPaaS) is also one of the very few growing segments of the telephony industry, and basically the only segment of the telephony industry characterised by innovation, with new use cases being developed every day. It is therefore important to ensure that the exceptions introduced in November 2022 work properly (there are concerns about Communications Providers treating the requirement of a pre-agreed interconnect as a way to increase wholesale charges, and there are concerns about excessive (intentional or inadvertent) blocking of calls that are in fact legitimate both according to the letter and the spirit of Ofcom's rules. Please also refer to paragraph 5.4 above, where blocklists and software tools deployed by Communications Providers are discussed. In case CLI authentication would be pursued in the UK, it must be done in a way to effectively address harmful activity, but also in a way which ensures that legitimate use is not unduly impeded, and in particular that rapid redress is available where legitimate use is impeded.

6.9 With regard to the concept of a 'gateway attestation' (paragraphs 5.44-5.48), Twilio reserves its position for possible future discussions. However, Ofcom and UK industry must be mindful of the fact that both CPaaS providers, and more traditional electronic communications network operators and service providers, are active in more than one country, and sometimes many countries, in addition to the UK. The specific position of multi-country Communications Providers must be adequately reflected in any envisaged arrangements.

6.10 The role and functions of a potential CLI Authentication Administrator are addressed in paragraphs 5.58-5.63 of Ofcom's document, as well as in Section 7. Based on its experience, notably in the United States, Twilio considers that strong governance arrangements are necessary to avoid dysfunctions and potential conflicts of interest between the certification authority on the one hand, and communications market participants on the other hand. More generally, the governance arrangements that appear to be essential to Twilio are the following:

(a) All willing Communications Providers should have the right to be involved, on equal terms, in defining both the technical aspects and the governance structure of CLI authentication to ensure that terms are not de-facto dictated by the largest Communications Providers. Ofcom would have to be actively present in discussions, with decision-making

powers, to ensure that both technical and governance arrangements are defined in a manner which does not negatively affect end-user interests and competition, and/or hamper innovation.

(b) In case Ofcom would in future come forward with proposals/proposed regulation to mandate CLI authentication, Ofcom's suggestions contained in paragraphs 6.5-6.7 seem relevant. Indeed, in a scenario where CLI authentication would be mandated, Twilio considers that the regulatory structure would have to be subject to strong Ofcom involvement, not only once the system is up and running, but also, and perhaps in particular, during the definition and the set-up phases of technical and governance arrangements. Enforcement powers for Ofcom, as envisaged by Ofcom, are indeed relevant. For example, the notion that Ofcom would be the entity able to take enforcement action in the event of non-compliance with the Administrator's rules (rather than the Administrator itself) (paragraph 6.7) is prima facie appropriate. Similarly, the notion that it would not be appropriate for the Administrator to impose sanctions on its UK members (paragraph 6.17), appears to Twilio to be a sensible suggestion. Ofcom's suggestion (paragraph 6.20) to the effect that the CLI Administrator would have no remit over the content of calls, also makes sense.

(c) A single certificate authority (the CLI Authentication Administrator) would logically be instituted, as Ofcom appears to be suggesting (paragraph 5.25), as well as an unequivocal boundary between the CLI Authentication Administrator function and any Communications Providers, not only in legal terms but also in practical terms. This is necessary to ensure that no undue preference or undue discrimination of Communications Providers occur.

(d) Costs would be apportioned in a manner which respects the differing sizes of Communications Providers in the UK. Agreeing a set of threshold values in terms of UK annual revenues and related financial contributions is likely a good way to approach this, as is promoting that the CLI Authentication Administrator and its suppliers would work based on a Software-as-a-Service model.

(e) The risk of false positives should explicitly be acknowledged and addressed in any formal regulatory measure, as well as in the technical and governance arrangements that would be applied. Therefore, prior to blocking being implemented, an agreed structured and efficient

process should be discussed for each case on a multi-lateral basis between Communications Providers. In addition, where blocking proves to be unjustified or accidentally impedes a legitimate use case, it should be possible for blocking to be undone immediately, and for more effective arrangements to be pursued. In particular, this entails going after the entity conducting harmful activity (harmful use may involve numbers that are also used for legitimate purposes, and may well go through multiple Communications Providers) rather than to block number ranges or even the traffic of a given Communications Provider.

(f) As Ofcom is no doubt aware, the UK telephony and messaging ecosystem is not only composed of electronic communications operators and service providers which originate and terminate calls/texts, but also involves smaller and sometimes companies with quite different characteristics. Those entities may act as resellers, distributors, system integrators, independent software vendors that provide solutions to businesses, etc. whilst not actually themselves being technically and/or commercially responsible for making the calls happen. In case CLI authentication is introduced, governance solutions need to create clarity on how calls facilitated or sold by such entities are treated. Twilio considers it necessary that Communications Providers can assist such entities, including for example by arranging the technical aspects of authentication on their behalf, with the appropriate trace-back arrangements being put in place.

7. Comments on Chapter 7: Implementation

Question 7.1: What are your views on the timescales for the potential implementation of CLI authentication, including the interdependencies with legacy network retirement?

Question 7.2: Do you agree with our assessment of the administrative steps required to implement CLI authentication and how these should be achieved?

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?

7.1 Twilio has limited additional comments to make on Chapter 7 at this time, given that Ofcom has not decided whether to come forward with proposals that would mandate CLI authentication in the UK. The key topics are already addressed by Twilio earlier in this response.

7.2 As regards timescales (Question 7.1, paragraphs 7.3-7.4), introducing CLI authentication is a large undertaking, for both the regulatory authority deciding to go forward, and for industry. Twilio expects that, even with the incorporation of learnings and potentially software solutions that are deployed or being deployed (notably in the US, Canada, and possibly France), a 24–36-month timeframe is the most rapid possible timeframe that can be envisaged. In addition, UK-wide implementation of IP-interconnection would, in terms of effectiveness, and in cost-benefit terms, be a prerequisite for introducing CLI authentication. Twilio also believes that it would not be wise to launch CLI authentication with partial/limited functionality, to be further developed after launch, as has happened in the United States and is planned in France. The reason is that the system will then almost inevitably perform below expectations, and sophisticated harmful actors will likely be able to reconfigure their activities to exploit remaining gaps in implementation.

7.3 On the topic of a common numbering database, Twilio confirms its position (see also paragraph 6.7 above) that a common number database (be it for Network Numbers only, or Network and Presentation Numbers) is not a prerequisite for implementing STIR/(SHAKEN) as a CLI authentication mechanism.

8. Comments on Chapter 8: Proposed framework for impact assessment

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.

8.1 Twilio has expressed its agreement with the objectives proposed by Ofcom (our paragraph 3.1 above) and explicitly welcomes the manner in which Ofcom is suggesting that an impact assessment could be conducted. This includes assessment of the counterfactual, the risk of negative impact if the proposed measures could result in some legitimate calls being blocked

(paragraph 8.15 of the impact assessment section), and other adverse impacts and potential unintended consequences (paragraph 8.21).

9. Role of CEPT ECC

9.1 Twilio notes that the CEPT ECC NaN working groups (in particular NaN1 (*future of numbering issues*) and NaN2 (*Number Portability and Switching, Trust in Numbering, and* Network *Technology Regulatory Issues*) have in the past addressed CLI spoofing, and are currently working on deliverables such as:

- draft ECC Report on Numbering for cloud-based communication services (NaN1 working group)

  https://cept.org/ecc/groups/ecc/wg-nan/nan1/client/meeting-calendar/

- draft ECC Recommendation on incoming international voice traffic with suspected spoofed national E.164 numbers (NaN2 working group)

  https://cept.org/ecc/groups/ecc/wg-nan/nan2/client/meeting-calendar/

This work is actively being pursued, with meetings scheduled, and consultations forthcoming. It would be unfortunate if individual authorities, such as Ofcom, would take radical decisions that will render a coordinated international approach impossible. Twilio appreciates that Ofcom is actively engaged in relevant discussions at CEPT ECC level and would welcome its continued efforts in ensuring that a common approach is taken in such a critical area.

10. Closing remarks

10.1 Twilio is available to discuss the matters at hand directly with Ofcom, to clarify its concerns, explain the legitimate use cases of its customers, jointly identify practicable solutions, etc. Please do not hesitate to reach out to:

Twilio Ireland Limited

Address: 3 Dublin Landings, North Wall Quay, Dublin 1, Dublin, Ireland D01 C4E0

Attention: Twilio Global Regulatory Affairs

Email: regulatory-notices@twilio.com