Craig Purdon
Comms Alliance
Via E-mail:

17 March 2022

Re: Scam Calls Code/Guideline

Dear Craig,

I am writing to you today on behalf of Twilio Inc (**Twilio**) as part of the consultation process on the draft Industry Code DR C661:2022 Reducing Scam Calls and Scam SMs (**Scam Code**) and the accompanying Industry Guideline DR G644:2022 Reducing Scam Calls and Scam SMs- Supplementary Information (**Scam Guideline**).

Domestically Originated Calls and Domestically Originated SMS.

Both in clause 4.2.1 (e) and clause 5.2.1(e) of the Scam Code, Twilio supports Option 2 which in both cases allows an Originating C/CSP to originate a call or SMS using a number that has been: issued to the A-Party by any C/CSP.

Allowing a customer to use a number that they have been issued by another C/CSP to originate a call or SMS is a common model already used in Australia and prohibiting the same will have a negative impact on customers and competition on the Australian telecommunications market. Customers have a legitimate expectation in Australia that CLI overstamping is allowed in Australia unless it is being done for an unlawful or malicious purpose. Twilio has experience in other jurisdictions that have managed to balance a customers' right to overstamp numbers that have been assigned to them by a carriage service provider (**CSP**) with regulatory requirements. In these jurisdictions where CLI overstamping is permitted:

- Twilio verifies that the customer has been granted a right to use the number by the issuing CSP;
- Customer data is uploaded into the equivalent of the IPND by the issuing CSP;
- Twilio can route the traffic originating from the number being used for CLI overstamping to the issuing CSP for termination; and
- Traffic terminating on the number being used for CLI overstamping will continue to be routed through the issuing CSP.

This arrangement could be utilised in Australia until such time as a more permanent solution could be found to allow customers to make flexible use of their CLI.

Twilio notes that other countries such as the UK allow for flexible use of CLI by allowing for a presentation number and network number method which requires that while all calls must be associated with a Network number that identifies the origin of the call, the CLI that is displayed to the receiving party, may be legitimately changed to another valid dialable number that uniquely identifies the caller.

Twilio notes that Ofcom has recently issued a consultation on further measures to reduce scam calls/scam texts and that its revised proposals do not include measures that would restrict a C/CSP from originating traffic for an A Party who is

using a number provided to them by another C/CSP. Indeed the revised text in the proposed changes to the CLI Guidelines that Ofcom has issued for consultation says in respect of a Presentation Number *"The originating CP is also responsible for ensuring that the Presentation Number satisfies the requirement that the CLI Data displayed within the call is a number that uniquely identifies the caller. The number must be either a CLI from a number range that has been allocated to the originating network, or the originating network should seek assurance from their customer that they are using a CLI that they have permission to use (either because they have been directly allocated that number or have been given permission by a third party who has been allocated that number)."*

This proposed revised guidance clearly places the obligation for validation on the originating provider but makes it clear that the presentation number that is displayed need not be a number assigned by the originating provider. In addition Ofcom has also indicated that it plans to issue a call for inputs in Q4 2022 on CLI authentication (*i.e.*, a STIR/SHAKEN approach) and what would be required to implement the technology across industry.

Twilio also notes that European Conference of Postal and Telecommunications Administrations (**CEPT**) has issued a public consultation on CLI Spoofing (Draft ECC Report 338) identifying "best practices" implemented by member states in order to combat CLI Spoofing. TThe report provides a recommendation on the approach national authorities should take to tackle CLI spoofing which includes:

1. an explicit prohibition of CLI spoofing, not only for operators but also for users, in national legislation;
2. the further elaboration of harmonised regulatory guidelines and/or mandatory rules in CEPT countries on how to deal with CLI spoofing;
3. to consider and to develop the roll-out of an European harmonised approach to call traceback (and call blocking)
4. the further analysis of technical methods such as STIR/SHAKEN, AB Handschake, SOLID, and Distributed Ledger Technology (*e.g.*, Blockchain) with the aim of eliminating CLI spoofing taking into account the following criteria:
    a. avoiding national fragmentation as much as possible;
    b. minimising the impact on the networks (*e.g.*, non-IP networks) and costs of implementation and management;
    c. ensuring compliance with EU- and national legislation on privacy;
    d. developments in other geopolitical regions;
    e. forward-looking potential of the choices to combat other types of fraud and abuse.
5. a coordinated roll-out of the chosen approach in CEPT countries (with STIR/SHAKEN being identified in the draft report as the preferred short/medium term solution CEPT members should focus their attention on).

Twilio notes that STIR/SHAKEN is therefore not only likely to be adopted across Europe and the UK in addition to being adopted in the USA. Twilio would therefore argue that as a more long term solution Australia should consider STIR/SHAKEN.

Internationally Originated Calls.

Clause 4.2.6 provides that "C/CSPs should not send Inbound International calls to B-parties on their own Telecommunications network or XPOI to the Transit C/CSPs or Terminating C/CSPs where the A Party CLI of an Inbound International Call is showing an Australian number unless exceptions apply (as per the Scam Guidelines).

The Scam Guidelines then says "In meeting the requirements of clause 4.2.6 of the Code there are some genuine call case exceptions. Below is a non exhaustive list of examples of these genuine calls case:

- As allowed under section 11 of the *Telecommunications (Telemarketing and Research Calls) Industry Standard 2017.*
- International mobile roaming
    - An Australian outbound roamer, in a foreign country makes a call to another Australian number.
    - An Australian outbound roamer received an incoming call from another Australian number, but a call forwarding condition resulted in the call coming back into Australia.
- Australian CSPs that provide SIP trunking services should closely monitor the CLI used by their customer, and investigate originating calls with a non-Australian CLI, unless there exists a prior written agreement for use of an international CLI.
- Offshore outbound call centres of Australian entities where the Australian entity has rights of use of the Australian number.
- Use of Unified Communications with domestic geographic numbers received from offshore.
- Satellite telephony call re-routing or other redirection."

Twilio supports the flexibility that is provided for in the Scam Guideline in relation to the fact that it is specified that the list of call cases is non exhaustive. Twilio also notes that in the equivalent section of the UK guidelines there are references to "*where the traffic has originated from UK customers that are hosted on overseas nodes or cloud service".* Twilio would suggest that a similar use case should be added to the Australian list.

Twilio remains at your disposal in the event that you require any additional information or clarification on our comments.

Yours sincerely,

Donald Connor

Donald Connor
Senior Director, Telecommunications Regulatory Compliance