RingCentral

11 March 2022

VIA EMAIL

Communications Alliance
Level 12, 75 Miller Street
North Sydney
NSW 2060

RE: COMMENTS TO C661:2022 *REDUCING SCAM CALLS AND SCAM SMS INDUSTRY CODE*

Dear Communications Alliance ("**CA**"),

RingCentral appreciates the opportunity to provide its comments to the revised draft Industry Code C661:2022 *Reducing Scam Calls and Scam SMS Industry Code* (the "**Revised Code**", and in its previous iterations, the "**Code**").

RingCentral is a global leader in the provision of business integrated communications and collaboration solutions over the cloud. We provide unified voice, video, team messaging and collaboration, digital customer engagement, and integrated contact center solutions to multinational business customers.

RingCentral appreciates the efforts of the CA to combat fraud in the new proposed section on preventing SMS Scams and the improved tracing and reporting measures in the Revised Code. CA's proposed prevention measures in the Revised Code effectively balance the need to minimize complexity and over-prescriptiveness, with public safety.

(Acronyms used below are as defined in the Revised Code)

RingCentral has the following comments:

1. In response to CA's request for comment on the alternate versions of clause 4.2.1(e), **Option 2** is the better approach.

    a. Option 2 meets customer's needs and facilitates business. There are legitimate reasons an A-Party would make calls with CLIs using numbers that were issued to the A-Party caller by a C/CSP which is not the originating C/CSP of those calls.

    b. Some of these reasons are:

        i. where an A-Party caller is awaiting a port to the originating CSP, because the A-Party has switched providers;

        ii. where an A-Party caller has purchased numbers in bulk; and

iii. where an A-Party caller is a business process outsourcing (BPO) provider making calls on behalf of its customers.

c. Notwithstanding these legitimate use cases, it is the obligation of service providers to ensure that we do not facilitate fraud by allowing this. It is important that the service provider takes reasonable efforts to prevent the use of a CLI where an A-Party caller does not have authority to use the telephone number as a CLI and wrongly impersonates the authorized entity.

d. To support this requirement, Cs/CSPs should be required to reasonably verify that their customers are authorized to use the telephone numbers they wish to display as CLIs.

e. RingCentral has long taken seriously its responsibility to safeguard the use of CLI, by consistently verifying that its customers are authorized to use any third-party provided CLI before allowing the use of these numbers as outbound CLI. RingCentral requires customers to provide proof of authority prior to substitution of CLIs, and periodically over time. The means of proof is straightforward – the Customer must provide an invoice from the provider of the subject telephone numbers dated no more than 30 days from the date of the Customer's request to substitute its CLI, and each subject telephone number must be listed on that invoice. This is then refreshed on a quarterly basis. RingCentral reserves the right to remove any number a customer uses as a CLI if the customer fails to prove its ownership of that number.

2. In response to CA's request for comment on the alternate versions of clause 5.2.1(e), **Option 2** is the better approach.

   a. Option 2 best meets customers' needs and facilitates business. There are legitimate reasons an A-Party customer of an originating C/CSP would send an SMS using a number which was issued to it by another C/CSP. These reasons are similar to those discussed above (paragraph 1.b).

   b. Just as above, it is important that service providers take reasonable efforts to prevent fraud.

3. RingCentral notes that the means of monitoring and tracing scam calls and SMs are not prescribed in the Revised Code. RingCentral appreciates this principle-based approach, for the following reasons:

   a. it allows industry participants to exercise their discretion in determining the appropriate level of implementation, and to abide by the spirit of the Code;

   b. it encourages innovation by the industry to find solutions to meet the need; and

   c. an overly-prescriptive approach is too transparent, and enables or encourages bad-actors to find loopholes and to out-innovate the prescribed measures.

4. RingCentral notes that ACMA[1] and CA[2] have each considered and briefly addressed the implementation of STIR/SHAKEN to combat scam calling. CA's concern at the time of its discussion paper was that "(STIR/SHAKEN) may prove difficult to implement in Australia due to Australia's combination of IP-based and legacy networks".

5. RingCentral has had a front-row experience with STIR/SHAKEN. We were an early-adopter, and by June 2021 had upgraded our entire network and implemented STIR/SHAKEN. We continue to be involved in the development of STIR/SHAKEN. A RingCentral employee sits on the Technical Committee that advises the US Secure Telephone Identity Governance Authority (**STI-GA**), which develops policies governing the use of SHAKEN certificates. Through industry groups, we actively participate in ongoing consultations with the US regulator on the implementation of rules governing STIR/SHAKEN and call blocking. RingCentral acknowledges the challenges which CA had pointed out in its May 2019 submission, and we wish to share our experience in that area:

    a. Many carriers in the US still rely on TDM in at least a portion of their networks, this is especially true of large, legacy carriers and smaller rural providers.

    b. When the United States mandated the implementation of STIR/SHAKEN, it noted and accounted for the differences in technology. Initially, the FCC required the implementation of the STIR/SHAKEN framework only to the IP portions of a carrier's network. After working extensively with the industry and other stakeholders, the FCC later mandated that all carriers must either (1) transition the non-IP portions of their network to IP or (2) develop a mechanism to authenticate calls in the existing TDM portions of their network.

6. Over the course of STIR/SHAKEN's implementation in the United States of America for some 10 months, RingCentral notes that the objectives of STIR/SHAKEN have generally been met:

    a. robocalls have been significantly reduced;

    b. there has been more reliability and security within our network;

    c. carriers have been forced to verify their customers, and to take responsibility for such verification. Carriers risk losing their STIR/SHAKEN certificate and ability to authenticate calls if they fail to verify the legitimacy of their customers and allow bad traffic to originate on their network.

[1] ACMA in its "*Combating Scams – Action Plan Summary*" dated November 2019
[2] CA in a joint submission with AMTA of "*Combating scams. A discussion paper on technological solutions*" dated 17 May 2019

Sincerely,

RingCentral Australia Pty Ltd

Director – APAC Corporate Counsel
RingCentral, Inc.