DRAFT REDUCING SCAM CALLS INDUSTRY CODE (DR C661:2020)

Twilio Comments
(8 May 2020)

Twilio welcomes the opportunity to comment on the Communication Alliance's draft *Reducing Scam Calls Industry Code* (DR C661:2020) (**Draft Code**).

About Twilio

Twilio is a global cloud communications service provider. Twilio's services allow enterprises to embed communications capabilities in their applications, enabling them to communicate more efficiently and effectively with their customers. Companies have used Twilio to allow users to contact their teacher or students, alert the public about an emergency, hail a ride, make a bank transaction, shop online, authenticate an account, and contact elected officials, among many other activities.

Founded in 2008 and headquartered in San Francisco, California, Twilio powers more than 800 billion interactions every year, and helps more than 190,000 customers globally – from small businesses to the world's largest multinational companies across many industries including education, healthcare, manufacturing, public safety, financial services – reinvent how they engage with their customers.

In Australia, since entering the market in January 2018, Twilio has grown from one employee to over 35 today in Sydney and Melbourne. Twilio's customers in Australia range from start-ups to some of the largest Australian companies, and come from a range of industries including financial services, food and hospitality, and logistics. To fulfill the growing local market demand for Twilio's services, Twilio is continuing to invest in sales, leadership, and support functions in Australia.

Statement of Interest

As a facilitator of trusted communications globally, Twilio takes seriously the threat that scam calls pose to customers and to the public at large, and actively participates in the fight against bad actors who place such calls. For example, Twilio has adopted a number of safeguards that prevent unlawful scam calls being placed through Twilio's services, including:
- requiring a customer to demonstrate that it has the right to use a phone number before allowing the customer to use the number as calling line identification (**CLI**) when initiating a call using Twilio's services;
- disabling calls to high-fraud destinations that are rarely used for legitimate use-cases, using a system of geographic permissions; and
- strong prohibitions, in Twilio's Terms of Service and Acceptable Use Policy, against using Twilio's services "*in connection with unsolicited, unwanted or harassing communications (commercial or otherwise), including, but not limited to, phone calls, SMS or MMS messages, chat, voice mail, video or faxes.*"

Twilio supports the objective of the Draft Code to address the problem of scam calls in Australia, and has a keen interest in contributing to its development. Twilio therefore offers the comments and recommendations below to aid the Communications Alliance in its further work on the Draft Code.

Twilio's Recommendations

In brief, Twilio's overarching recommendations are that:

- there should be a **central web portal for consumer education** on scam calls;
- the Draft Code should clarify that **legitimate CLI masking** is permitted;
- the Draft Code should include a **dispute resolution mechanism**; and
- the Draft Code should require **good faith implementation** of its requirements by carriers and carriage service providers (**C/CSPs**).

Details of these overarching recommendations, and Twilio's recommendations on specific clauses of the Draft Code, are below. Unless otherwise indicated, acronyms and capitalised terms used below bear the same meanings as in the Draft Code.

1.   Overarching Recommendations

1.1 Central Web Portal for Consumer Education

Twilio's Recommendations:
- There should be a central web portal, managed by the Australian Communications and Media Authority (**ACMA**) or another independent body, to provide consumers up-to-date guidance on scam calls.

Rationale:
Twilio supports having consumer education on scam calls. However, as scam call perpetrators constantly update their methods to more effectively target and defraud unsuspecting end-users, it would be difficult for C/CSPs to maintain up-to-date consumer guidance materials, as required under Draft Code clause 3.1. This in turn risks C/CSPs being in breach of Draft Code clause 3.1, despite efforts to comply. Having different, and potentially conflicting and outdated, sources of guidance on scam calls from different C/CSPs also risks confusing consumers on what exactly to look out for.

Having a central web portal that consumers can visit for guidance on how to deal with scam calls would help to avoid these problems. Instead of the Draft Code requiring C/CSPs to maintain separate consumer guidance on their own websites, the Draft Code could provide that C/CSPs only need to voluntarily contribute information to an independent body, such as ACMA, to consolidate and update the central web portal. Given its public-service nature, the costs associated with setting up and maintaining the central web portal should be borne by the Australian government. Relating to this, ACMA already has a site providing consumer education on scam calls that could be expanded to serve the function of a central web portal.[1]

1.2 Legitimate CLI Masking

Twilio's Recommendations:
- The Draft Code should clarify that legitimate CLI masking is permitted, by using the term "Illegitimate CLI Spoofing" and excluding legitimate CLI masking scenarios from the definition of that term.

---

[1] See ACMA's site on phone number scams at: https://www.acma.gov.au/phone-number-scams. Several other jurisdictions also have such central web portals for consumer guidance on scam calls, e.g., New Zealand's Netsafe (https://www.netsafe.org.nz), Singapore's Scam Alert https://www.scamalert.sg, and the site of UK's telecommunications regulator (Ofcom) (https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/problems/tackling-nuisance-calls-and-messages), funded by New Zealand, Singapore, and UK governments (respectively).

Rationale:

CLI masking is legitimately used to maintain user privacy and to enable users to have a trusted means of communications where they prefer not to share private information like their telephone numbers. Examples include legitimately modifying displayed telephone numbers in conversations between drivers and riders on ride-sharing apps, and messages from health counselling services to home phone numbers. Such CLI masking is legal in Australia[2], and the above recommendations would clarify that the Draft Code does not prohibit such CLI masking.

1.3 Dispute Resolution Mechanism

Twilio's Recommendations:

- The Draft Code should include a dispute resolution mechanism, the details of which should be further discussed and agreed among all relevant stakeholders.

Rationale:

Having a mechanism to resolve disputes on scam calls fairly and expeditiously – including disputes with respect to a C/CSP blocking legitimate calls from another C/CSP, or unreasonable requests being made by one C/CSP to another – would be key to the effectiveness of the Draft Code. The details of the dispute resolution mechanism should be discussed and agreed among all relevant stakeholders. These details should include how disputes are to be raised and to whom, the timelines for response and decisions on the dispute, and the party or parties responsible for bearing the costs of the dispute resolution.

1.4 Good Faith Implementation of Draft Code

Twilio's Recommendations:

- The Draft Code should require all C/CSPs to implement and discharge their responsibilities under the Draft Code in good faith.

Rationale:

While well-intentioned, the Draft Code could conceivably be used by C/CSPs to harm their competitors, ultimately to the detriment of competition and consumers in Australia. For example, Draft Code clause 4.7.4 requires an International Operator to act as soon as practicable to stop the delivery of further scam calls from CLIs identified by a C/CSP, failing which all of the International Operator's calls could be blocked in Australia. However, there is nothing to prevent a C/CSP from flooding a competing International Operator with bad-faith requests to stop the delivery of scam calls (some or all of which could be legitimate), requiring the International Operator to expend an inordinate amount of resources to deal with the requests, or risk being blocked. A requirement for C/CSPs to act in good faith, coupled with the dispute resolution mechanism recommended above, would help to ensure that the Draft Code is appropriately and effectively implemented.

2. Recommendations on Specific Draft Code Clauses

2.1 Draft Code Clauses 4.1 and 4.2

Twilio's Recommendations:

- Draft Code clauses 4.1 and 4.2 should **both** emphasize that "*legitimate phone calls (including telemarketing calls) can also exhibit the same characteristics as Scam Calls*", and that C/CSPs should consider the full circumstances at hand (instead of only the criteria and

---

[2] See the section on "CLI overstamping" on ACMA's site at: https://www.acma.gov.au/phone-number-scams.

indicators mentioned in the Draft Code), and also consult the relevant transit/originating C/CSPs, before determining that calls are scam calls.

Rationale:

Twilio commends the Communications Alliance for noting in Draft Code clause 4.2 that "*legitimate phone calls (including telemarketing calls) can also exhibit the same characteristics as Scam Calls.*" Indeed, there is a broad range of legitimate calls that display similar characteristics as scam calls (e.g., calls from mass notification systems to communicate essential information during times of crisis; calls from ride-sharing, reservation, delivery, and other legitimate services to provide notifications and updates to customers; and 2-factor authentication calls). The above recommendations would help to reduce the instances of legitimate calls being falsely labelled as scam calls.

2.2   Draft Code Clause 4.3.1

Twilio's Recommendations:
- Draft Code clause 4.3.1(b) should be amended to read "*transferred or allocated to them via a 3rd party C/CSP contractual relationship, or hosted by them on behalf of another C/CSP*".
- A new provision should be inserted, possibly as Draft Code clause 4.3.1(d), that allows for call origination using numbers "*verified by the relevant A-Parties as numbers that they have the right to use for originating calls*".

Rationale:

Draft Code clause 4.3.1 currently permits C/CSPs to originate calls using only numbers that are: (a) directly allocated to them by ACMA; (b) transferred under a third-party C/CSP contractual relationship; or (c) ported in from another C/CSP. The above recommendations seek to clarify that other legitimate call-origination scenarios are permitted, such as where the C/CSP is hosting a number that has been directly allocated by ACMA to another C/CSP (e.g., where the latter C/CSP does not have a physical network to host the numbers), and where the customer in question has the right to use the number (e.g., through a contractual relationship between the customer and a third-party C/CSP).

2.3   Draft Code Clauses 4.4.2 and 4.4.5

Twilio's Recommendations:
- The note under Draft Code clause 4.4.2 (stating that each C/CSP "*is responsible for determining how they monitor their networks to detect Scam Calls on their networks*") should be moved to Draft Code clause 4.4.1; and the remainder of Draft Code clause 4.4.2, and the related Draft Code clause 4.4.5, should be deleted.

Rationale:

Draft Code clause 4.4.2 requires C/CSPs to monitor their networks using a very specific indicator, i.e., CLIs received from other C/CSPs. This could require a receiving C/CSP to dedicate significant (and potentially unnecessary) financial and manpower resources, for a potentially unlimited duration of time, to track the usage of particular CLIs notified to it, which may or may not be CLIs used for scam calls.

A better position would to require C/CSPs to perform ad hoc investigation and remediation of scam calls based on CLIs that are notified to them by regulators or in good faith by other C/CSPs, and to allow C/CSPs to implement their own processes and rely on their own data points to monitor scam calls, as already contemplated under Draft Code clause 4.4.1 and the

note under Draft Code clause 4.4.2 mentioned above. The above recommendations would implement this position.

2.4 Draft Code Clause 4.6.4

Twilio's Recommendations:
● The Draft Code should include guidance or criteria on how to determine when a Public Number is no longer used for scam calls.

Rationale:
Draft Code clause 4.6.4 requires C/CSPs to take action to unblock a Public Number where the Public Number is found to be, among others, no longer used for scam calls. However, it is unclear how one would determine when a number is no longer used for scam calls – as, when a number is blocked, that number can in fact no longer be used for scam calls.

2.5 Draft Code Clause 4.7

Twilio's Recommendations:
● International Operators should also have recourse to the dispute resolution mechanism (recommended in section 1.3 above) to ensure that legitimate calls from the International Operators' networks are not blocked by C/CSPs.

Rationale:
Draft Code clauses 4.7.1 through 4.7.8 set out a process for a C/CSP to ask an International Operator to block scam calls coming from the International Operator's network. Where the International Operator fails to block the calls, all C/CSPs in Australia can block calls from that International Operator after a notice is issued to the International Operator and the International Operator "*fails to respond*" to the notice. Where the International Operator is "*no longer uncooperative or unresponsive*", the C/CSPs must unblock the International Operator.

The Draft Code's requirements in this regard are rigid and do not take into account scenarios where the International Operator may legitimately refuse to block the calls in question, for example, where the International Operator has itself ascertained that the calls are legitimate, or where the blocking request was made without sufficient details, or even where the International Operator is faced with a flood of bad faith requests and inadvertently fails to respond to one or more of such requests.

The ability to block calls is a drastic measure that could affect legitimate incoming calls to Australia, and also the legitimate businesses of International Operators. Access to the dispute resolution mechanism recommended in section 1.3 above would allow an International Operator to resolve issues of legitimate incoming calls to Australia being blocked.

2.6 Draft Code Clause 5.1.2

Twilio's Recommendations:
● Draft Code clause 5.1.2 should be amended for clarity as follows:
  "*Each C/CSP~~s~~ must complete, maintain and keep up to date, ~~an industry contact~~a list of its contacts and provide the list, and any updates to the list that may be made from time to time,~~their details~~ to CA. ~~C/CSPs must maintain and keep the contacts current.~~*"

Rationale:

The above recommendations would clarify that a C/CSP needs to maintain a list of only its own contacts (that other C/CSPs and/or the ACMA can contact for purposes of the Draft Code), and not a list of all contacts throughout the entire industry.

Conclusion

While the Draft Code is a good and important starting point for addressing scam calls in Australia, Twilio recommends that there be a broader and continuous industry discussion on other possible mechanisms that could be deployed to ensure a more complete solution to the problem. One such mechanism could be the STIR/SHAKEN framework adopted in the US.[3] Another possibility would be to have a neutral body centrally co-ordinating anti-scam-call efforts among all relevant stakeholders, including law enforcement, communications providers, and communications and consumer protection authorities.[4]

Twilio appreciates the opportunity to comment on the Draft Code and would welcome the opportunity to discuss and participate in the Communications Alliance's further work on the Draft Code and on addressing scam calls in Australia.

---

[3] Secure Telephone Identity Revisited (**STIR**) and Signature-based Handling of Asserted Information Using toKENs (**SHAKEN**). STIR/SHAKEN is a call-authentication framework that allows the recipient of a phone call to know if the caller has the right to use the CLI by displaying a green checkmark or similar indicator, bringing the same feeling of trust when one sees a lock next to the URL in a web browser. For further details of STIR/SHAKEN, please see the FAQs maintained by the Alliance for Telecommunications Industry Solutions at: https://www.atis.org/sti-ga/resources/docs/shaken-faqs.pdf.

[4] The Industry Traceback Group (**ITG**) in the US (https://www.ustelecom.org/the-ustelecom-industry-traceback-group-itg/) would be an example of such a neutral central coordinating body. The ITG is a collaborative effort of companies across the wireline, wireless, VoIP and cable industries to trace and identify the source of illegal robocalls, and to coordinate with law enforcement agencies for appropriate enforcement action. New Zealand's Netsafe (https://www.netsafe.org.nz) and Singapore's Scam Alert https://www.scamalert.sg are also examples of central bodies for coordinating anti-scam-call efforts among law enforcement, communications providers, and other stakeholders.