Consultation: Existing Consumer Authentication Code

Twilio's Response to the Consultation by Communications Alliance on DR C666:2021 Existing Customer Authentication Draft Code

20 September 2021

1. About Twilio

1.1 Twilio is a leading global CPaaS (Communication Platform as a Service) provider and is a registered carriage service provider within the meaning of section 87 of the Australian Telecommunications Act.

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

1.4 Other customers include international brands but it should be noted that many of Twilio's customers are also small and medium-sized enterprises and Twilio's non-profit arm, Twilio.org, supports charitable organizations to deliver their communications needs.

1.5 Please do not hesitate to refer any questions or remarks that may arise as a result of our comments to Twilio Global Regulatory Affairs at the email address regulatory-notices@twilio.com

2. Twilio's Comments

2.1 Twilio welcomes the opportunity to provide feedback to the Communications Alliance on the consultation on DR C666:2021 Existing Customer Authentication Draft Code.

2.2 Twilio appreciates that the Code C666:2021 will work in concert with other regulatory safeguards, including the Pre-Port Verification Standard and the Reducing Scam Call Industry Code, to seek to minimise scamming and fraud for all Australian telecommunications users.

2.3 Twilio service platforms and processes have been designed with end user security at its core and leverages strong multi factor authentication measures to protect not only Twilio's customers but all Australian telecommunications users. Twilio welcomes this self-regulation initiative by industry aimed at supporting the use of customer authentication measures to further limit fraudulent activity on accounts of residential and small business customers.

2.4 The proposed Code will play a critical role to develop a set of coordinated principle applicable to the entire industry and Twilio welcomes the opportunity of contributing to

its further development of the Code and its implementation by joining the drafting working group.

2.5 Twilio has the following observations on the proposed Code:

A. Section 3.2.1 (Risk Based Activities) of the states that "*Customer service approaches must consider what information may be publicly accessible and how that may be used by those with criminal intent to access a customer's service*." Twilio's belives that it will be quite important to specify what "publicly accessible" entails for the purpose of the Code, and whether for instance this extends to data that may be available on social media platforms and excludes any data not generally available to the public, for instance including data that may be "available" on the dark web following data breaches.

B. Section 3.3 of the proposed code (Multi Factor Authentication) the code states that a first authenticator must be a knowledge authenticator that is not publicly available) and that only the Customer should know (Section 3.3.1) and that further authenticators must be a Biometric Data method or a possession authenticator In Twilio's view this latter may require further considerations before implementation given wider policy implications and likely operational difficulties associated with such implementation for smaller CSPs.

C. Section 3.2.5 requires CSPs to ensure that all high-risk transactions are secured using Multi Factor Authentication or other appropriate security measures. Twilio notes that there is no complete clarity as to what constitutes a high-risk transaction. Whilst accompanying guideline (G688:2021) provides examples they are are open-ended list of examples. Twilio urges that a definite list of what constitutes high-risk transactions be developed by the Communications Alliance in order to provide full clarity to CSPs on what transactions are to be considered as high-risk.

3. Conclusion

The proposed Code will play a critical role in the further development of a coordinated industry approach to customer authentication and Twilio will welcome the opportunity of contributing to its further development of the Code and its implementation by joining the drafting working group.