



New Rules to Prevent Fraud From Unauthorised Customer Interactions with Telecommunications Providers (Proposal to Make the Telecommunications Service Provider (Customer Identity Verification) Determination 2021

Twilio's Response to the Consultation by Australian Communications and Media Authority

15 December 2021



1. About Twilio

- 1.1 Twilio is a leading global Communication Platform as a Service (**CPaaS**) 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 Twilio welcomes the opportunity to provide feedback on the Australian Communications and Media Authority's Consultation: New Rules to Prevent Fraud From Unauthorised Customer Interactions with Telecommunications Providers (Proposal to Make the Telecommunications Service Provider (Customer Identity Verification) Determination 2021 (**Draft Determination**)).
- 1.6 Please do not hesitate to refer any questions or remarks that may arise as a result of our comments to Twilio's Global Telecommunications Team at the email address regulatory-notice@twilio.com

2. Twilio's General Comments

- 2.1 Twilio respectfully suggests that the Australian Communications and Media Authority (ACMA) Draft Determination is unnecessary given the co-existence of the Communications Alliance code C666:2021 Existing Customer Authentication (**CA Code**) which is currently before ACMA for registration. Industry has spent many hours developing the CA Code and Twilio believes that the introduction of ACMA's Draft Determination before the CA Code has been registered and can be put into practice risks undermining the willingness of industry to come together and work on similar issues in the future.
- 2.2 Similarly, Twilio notes that the CA Code having been put together as a result of industry discussions and having had detailed input from carriage service providers who understand their customers, how their customers interact with them on different type of transactions and how their support systems work is far less prescriptive than the ACMA's Draft Determination. It is this very prescriptive nature of the Draft Determination that at best makes ACMA's proposal incredibly costly to implement and at worst makes the proposal totally unworkable all without protecting customers from harm.



- 2.3 While Twilio appreciates that the ACMA wishes to protect consumers from harm and supports such measures, the Draft Determination's one size fits all approach is based on implementing rules that are commendable for a mass consumer product involving consumers interacting with carriage service providers through call centers. This one size fits all approach does not take into account that many carriage service providers also serve business customers through account management teams where the identity of the customer is known as a result of personalised relationships.
- 2.4 Simply put the Draft Determination cannot be implemented practically by carriage service providers, such as Twilio, that predominantly serve large business and enterprise customers and multinational enterprises. Such customers have account managers and account management teams that engage in weekly if not daily interactions with representatives of the company to discuss their accounts and provide reports. In accordance with the Draft Determination, any carriage service provider that adopts similar support mechanisms for such customers would be required to engage in two factor authentication of the type set out in the Draft Determination in sending out these reports or interacting with representatives of the companies merely because in discussing the customer's services they may be "disclosing any **information held by the carriage service provider relating to the customer's account** including personal information or business information." (emphasis added) .
- 2.5 The reality is that such transactions poses no risk to the customer, let alone a high risk. It does, however, reveal the fundamental flaw of the Draft Determination in that the definition of high risk customer interaction is far too broad and takes no account of how different types of customers particularly enterprises or large businesses interact with their carriage service providers and what transactions and interactions might actually pose a risk to them. This when combined with a one size fits all multi-factor authentication (**MFA**) process that must be followed for every transaction that falls within the extremely broad definition of a high risk transaction means the Draft Determination has immense overreach.
- 2.6 Twilio notes that the Draft Determination makes no reference to the use of a Systems Integration Channel as an alternative option to the MFA. This is in sharp contrast to the CA Code which provides that "CSPs must ensure all High Risk Transactions are secured via Multi Factor Authentication or by a Systems Integration Channel. High Risk Transactions are secured via Multi Factor Authentication or by a Systems Integration Channel." The CA Code defines a Systems Integration Channel as "the use of APIs (Application Programming Interfaces) or a similar agreed electronic data exchange layer for the purposes of enabling machine to machine integration between a Large Business Customer system and a Carriage Service Provider system.
- 2.7 Twilio fully supports the use of a systems integration channel as an alternative method of authentication for all customers not just large business customers. Twilio believes that by limiting systems integration channels to large business, small and medium size businesses will be denied technology available to their larger rivals to the detriment of innovation and the



Australian economy. The vast majority of Twilio's smaller business customers use APIs to carry out transactions with Twilio such as purchasing telecommunication services. APIs will continue to grow in use and Twilio would urge ACMA to recognise them within the Draft Determination as an alternative MFA method for all customers in Australia

- 2.8 Twilio also urges ACMA to reconsider the timing for implementation. Carriage service providers are currently faced with a situation where they do not and will not have certainty for some time as to whether the CA Code or the Draft Determination will apply. Carriage service providers cannot therefore begin to put into place the tools to meet these requirements until they have this certainty. In addition, even when carriage services providers have certainty over the requirements, carriage service providers such as Twilio will need to engage in re-engineering processes and make any necessary system changes as well as training staff on the new process. Twilio notes that for many providers there would be a need to find, contract and implement a MFA solution. All of this work could take anywhere between twelve and eighteen months. As such, the proposed implementation date in the Draft Determination of April 2022 is completely unrealistic.

3. Twilio's Response to ACMA's Questions

- 3.1 In this section Twilio sets out its comments on the questions posed by the ACMA on the Draft Determination. Twilio's decision not to respond to any particular question raised by ACMA does not necessarily represent agreement, in whole or in part with the Draft Determination. Twilio does not directly address all of the ACMA's questions but uses those as a framework for providing comments on the Draft Determination.

Are the customer identity verification requirements adequate to achieve the objectives of the draft determination to reduce consumer harm and protect the security of high risk customer interactions

Will the definition of high risk customer interactions capture all of the interactions targeted by or vulnerable to scammers? If not what are the other interactions?

Are there any specific interactions or class of interactions that should not be considered high risk and why?

- 3.2 Twilio notes that much of the commentary by the ACMA in the consultation focuses on the harm to consumers from identity fraud over telecommunications networks which has primarily occurred in two-ways. One is unauthorised mobile porting (now addressed by the Mobile Porting Verification Standard) and the other is unauthorised SIM swap. The consultation also says that scammers have used personal information to facilitate other types of fraud such as "purchasing" expensive handsets on a customer's account or gaining full access to customer accounts and payment details. The document says that "*consumers who are the victim of*



identity theft typically suffer both financial loss and psychological harms. The effects can be life altering, impacting health, emotional wellbeing and relationships with others.”

- 3.3 The consultation, however, offers no real evidence of business customers suffering harm from any particular types of transactions. As such it is not clear what ACMA's objectives are in relation to business customers and how the proposed legislation is either evidence based or proportionate in its application to them. This is important because the definition of high risk customer interaction applies to all customers, including business and government customers.
- 3.3 This is in marked contrast to the CA Code. In the CA code the definition of high risk customer transaction focuses on the likely outcome to the customer with a note providing some examples of what constitutes a high risk customer transaction.

“High risk customer transaction means any transaction that may result in one or more of the following outcomes:

- (a) The Customer losing access to their Telecommunications Service;*
- (b) A change to any information held or acknowledged by the CSP as relating to the identity of the Customer and*
- (c) charge is applied or will be applied to the Customer’s account.”*

Note. High risk transactions include but are not limited to:

- *SIM swaps;*
- *Viewing or changing unique internal identifiers, customer name, DOB, email, password, payment or contact details;*
- *Changing an authorisation access method (eg PIN, password, IMEI or IMSI);*
- *Enabling call diversion;*
- *Enabling call barring; and*
- *Purchases over a defined limit.”*

- 3.4 The CA Code requires a carriage service provider to designate High Risk transactions based on whether *“the transaction relates to a Consumer or Large Business Customer and what will be the impact of the associated transaction and the potential risk of harm to the Customer of the transaction.”*
- 3.5 The ACMA's Draft Determination of high risk customer interactions, however, as discussed above is one size fits all.

*“High risk customer interaction means an interaction relation to a customer’s telecommunications service, instigated by either the requesting person or by the carriage service provider, where the carriage service provider does all or **any** of the following:*

- (a) Adds or removes a telecommunications service from a customers account or modifies an existing telecommunications service; or*



- (b) *Modifies **any information** held by the carriage service provider relating to the customer's account including personal information and business information; or*
 - (c) *Discloses **any information** held by the carriage service provider relating to the customer's account including personal information and business information including but not limited to "a SIM swap request, a call diversion or call forwarding request, a request to transfer a telecommunications service from being a postpaid carriage service to a prepaid service and a call barring request, but does not include a transaction to port a mobile number to which the Telecommunications (Mobile Number Pre Porting identity Verification) Industry Standard 2020 applies."*
- 3.6 The use of the word 'any' in the definition without any qualifier means that a number of activities where no risk of harm would be posed will be caught, even activities that may be covered by other codes or legislative provisions such as the Telecommunications Consumer Protection Code or the Numbering Plan.
- 3.7 This is heightened by the fact that the Draft Determination captures transactions that are initiated by the carriage service provider as opposed to the CA Code which focuses on transactions undertaken by a person who is contacting the carriage service provider to:
 - a) Undertake a transaction in relation to a telecommunications service; or
 - b) Gain access to information relating to a telecommunication service.
- 3.8 As the Draft Determination currently stands, were ACMA to withdraw a numbering range and require carriage service providers to recall and replace those number from their customers accounts, the mere act of communicating that information to the customer by email or letter would appear to fall within the scope of a high risk transaction because it is a disclosure of information about the customers account including that they have that type of number and the actual removal and addition of replacement numbers from the customers account to meet the ACMA requirement would also constitute a separate and distinct high risk transaction as it removes and then adds a telecommunication services from the customer accounts.
- 3.9 Twilio suggests, and hopes that ACMA agrees, that this is not a high risk customer interaction and it should not be the subject of the prescriptive MFA outlined in the Draft Determination. Indeed it is not clear that either of the two steps could practically be subject to MFA as outlined in sections 9 and 10 of the Draft Determination.
- 3.10 Indeed it is not clear how any outbound written communications that are sent, or to use the language of the Draft Determination's instigated by a carriage service provider can be subject to a MFA authentication process as set out in sections 9 and 10 despite the fact that almost all of these communications will fall within the definition of disclosure of information that is addressed to the customer (thus disclosing personal information in that they will contain the customer's name and address or business information the business name and address) as well as other information about their account.
- 3.11 Twilio suggest, and hope that ACMA agrees, that it is clearly not feasible to require that the sending of a bill by post or email to a previously verified address nominated by the customer be subject to a MFA process as set out in the Draft Determination.
- 3.12 Twilio cites these examples as only some examples of the interactions that are caught up in the



wording of the Draft Determination despite there being no risk of customer harm. Others include sending a renewal notice in relation to a customer contract, sending a notice of breach or termination under a contract, sending of outage notices, renewal discussions between an authorised representative and account executives, a meeting between a representative of an enterprise customer and employees of the carriage service provider where aspects of the account are discussed.

- 3.13 All of these fall within the very broad definition of a high risk transaction which **must then** be subject to the identify verification processes set out in section 9 and 10 of the Draft Determination as applicable. The likely risk of harm to the customer from the list of activities above is low and Twilio respectfully suggests that it neither feasible or necessary to classify such transactions as high risk nor to apply MFA to the type of interactions set out above and many other interactions with customers that occur on a daily basis.
- 3.14 Twilio urges ACMA if it does press ahead with its own determination to reconsider its approach to defining a high risk transaction to ensure that the focus is on the harm that might be caused by a particular transaction arising from a requesting person and to allow carriage service providers to identify these transactions themselves. This would allow carriage service providers to take into account the very many different customer types they serve and the products they provide them. Providers who do not serve consumers and who do not provide mobile devices will have far fewer circumstances where transactions are likely to be high risk in the sense of causing financial loss to a customer or involving a risk of a customer losing their service or having information that might cause them loss disclosed.
- 3.16 Twilio believes that it is not an issue of merely taking an approach of leaving the definition as is and carving things out of the definition of high risk interaction. Rather the approach should be fundamentally realigned to allow carriage service providers who know their own customer base and products best to define what are high risk transactions for their customers and products.

ACMA is specifically interested in how the proposed process will work where authorised representative arrangements are in place.

- 3.17 Twilio experience with this question is limited to the authorised representatives of companies. The current process as set out in section 9 of the Draft Determination is not workable in all situations. Take for example circumstances where there is a relationship between the representative of a company and an account executive and the authorised representative is requesting to discuss their account or even to make a change to their service directly from that account executive in the context of a conference call, video conference call or a face-to-face meeting.
- 3.18 Is it necessary to request that the representative go through the identity verification process outlined in section 9(1) of the Draft Determination and then follow this up with one of the processes set out in section 9(2). Even the supposed process that deals with large business customers in section 9(2)(d) of the Draft Determination is not tailored to the realities of large business accounts. There may be a number of services being provided by a carriage service provider and a number of people who are authorised by the customer to deal with that account but the number that is listed on the account as a contact number may not belong to any of these authorised parties. For example, the IT department may be responsible for international



broadband connectivity while the facilities department may be responsible for plain old voice telephony services.

- 3.20 Twilio once again urges ACMA to not impose processes designed for dealing with consumers on carriage services providers dealing with a far more diverse range of customers who in many cases have contracted for their own specific levels of customer service and arrangements for dealing with their accounts.
- 3.21 In this respect, Twilio notes that it is not uncommon for exemptions to be granted to providers serving large business customers. Indeed the FCC has granted an exemption for large business, enterprise and government customers in the new FCC Rules to prevent SIM swapping and Port Out Fraud and its related business customers exemption. The FCC exemption states; “Business customer exemption: Telecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide specifically to their business customers that have both a dedicated account representative and a contract that specifically addresses the carrier’s protection of CPNI.”¹

Are there additional examples of account information, personal information or possession based authenticators that should be covered by these definitions?

The draft determination imposes a time limit of one day for multi factor identity verification to be completed using identity documents. Is a time limit required and if so, is this period appropriate?

Are there additional processes that should be considered for customers in vulnerable circumstances?

ACMA is specifically interested in how the proposed process will work where authorized representative arrangements are in place.

- 3.22 Twilio notes that section 11 of the Draft Determination deals with identity verification requirements for customers in vulnerable circumstances. The requirement is that if a carriage service provider suspects that a requesting person is a customer in vulnerable circumstances then, an employee or agent who has completed fraud mitigation training must use the process set out in the section. Twilio is deeply concerned that it may not be until a carriage service provider’s representative has accessed a customer’s account that they will have the information at hand to understand that the customer is in vulnerable circumstances and to arrange for a staff member with fraud mitigation training to deal with the matter. Otherwise this means that staff members are being asked to make assumptions that may be wrong at the very outset of their dealings with customers as to whether they are vulnerable without having regard to information that may be on the customer’s account. Twilio is concerned that this is likely to lead to potentially stereotyped and potentially discriminatory judgements being made. Also surely

¹ Customer Proprietary Network Information



these requirements cannot apply to circumstances where a customer is carrying out a transaction online on their account as the carriage service provider will not know that the transaction is occurring. Twilio is also concerned about the requirement to monitor the account for 30 days.

- 3.23 Again it is the prescriptiveness of these requirements that concerns Twilio. Carriage service providers who have day-to-day experience dealing with vulnerable customers should be in the best position to design the processes that should apply to vulnerable customers once it is understood that the customer is vulnerable.

ACMA is seeking feedback on the timing of commencement of the determination including on any staged transitional arrangements that could be considered so that consumer protections are in place as quickly as possible.

- 3.24 As set out above, Twilio suggests that the 5 April 2022 date is unrealistic. As a provider offering services to multinational customers (as opposed to a provider who only has Australian customers) some of whom may take Australian services, Twilio will need to examine all of its communications and customer channels and design process and system changes to ensure that it is able to meet the final requirements when those are known. Twilio thinks that realistically Twilio would need 12 to 18 months, in order to be able to do the discovery work, re-engineer its systems and processes and train its staff to deal with those new processes and systems.

4. Additional Comments on the Draft Determination

- 4.1 Twilio notes that the elements of the MFA process outlined in section 9 of the Draft Determination are also extremely prescriptive. In particular, even the use of a unique verification code is set out in a very prescriptive manner including the requirement to include in the message in which the unique verification code is sent a clear statement informing the customer:
- (A) of the reason why the code is being provided;
 - (B) that the code should not be share with any other party except the carriage service provider if the customer has requested the high risk customer interaction; and
 - (C) what the customer can do if they did not authorise the high risk customer interaction .
- 4.2 Twilio notes that when a customer is logging into an account, the carrier services provider will only know that there is a login and not any other reason behind this. Again Twilio wonders whether the prescriptiveness of A, B and C is required. Similarly if a customer representative is speaking to a customer they will not know the reason for the transaction until the customer has been authenticated.



- 4.3 Similarly section 9 2(b)(iii) of the Draft Determination provides that “after the receipt of [unique verification code] by a customer, the carriage service provider receives immediate confirmation from the customer via the same means by which the unique verification code was sent for the purposes of subparagraph (i) that the customer has received the unique verification code.
- 4.4 Twilio does not understand why the unique verification code must be confirmed in the same way that it was sent. It is extremely common for customers who are logging in on a platform and having a unique verification code sent to further authenticate them to have the choice of a number of methods of having that code sent (text, email) and then input that unique verification code into the platform.
- 4.5 What is important is that the carriage service providers are able to confirm that the customer has received the unique verification code. Twilio would urge ACMA to remove the prescriptiveness from this provision.
- 4.6 Twilio also notes that section 12 of the Draft Determination is not clear. Section 12(1) provides that if a customer requests a carriage service provider to use an additional identity verification process prior to undertaking any higher risk interaction in relation to that service, the provider must comply with the request until the request is canceled by the customer. An additional identity verification process means in addition to the requirements in section 9 of the Draft Determination, the use of one more (a) account information authenticator, (b) personal information authenticator or (c) identity verification process described in section 9(1) where the information or process has not already been relied on for the purpose of complying with the requirements in section 9.
- 4.7 Twilio notes that there is no need for such a request in section 12(1) of the Draft Determination to be reasonable and the requirement to comply is absolute. However adding in an additional identity verification process will potentially mean re-engineering processes and potentially systems and retraining customer service staff. This needs to be done at no cost to the customer in accordance with section 14 (d) of the Draft Determination.
- 4.8 Section 12(2) of the Draft Determination goes on to state that if a customer makes a valid request to a carriage service provider who provides their telecommunication service to only process a high risk customer in relation to that service in the manner specified by the customer, the provider must comply with that request. A valid request is defined in section 12 (3) as a request that (a) specifies the identity verification process that should be used prior to the carriage service provider undertaking the high risk customer interaction and (b) specifies where that process must be undertaken in a retail environment, online or in a call centre environment, where at the time of the request, the carriage service provider is using the requested identify verification process in the environments requested for the purpose of complying with this determination. Again no cost can be charged for this and there is no requirement for the request to be reasonable in the context of the customer itself and the services it is taking.



- 4.9 Twilio is not clear how section 12(2) of the Draft Determination should be understood. Does 12(2) of the Draft Determination and its use of the word “only” mean that the distinction between 12(1) and 12(2) is that customers can use section 12(1) to request an additional verification process on an ad hoc basis and section 12(2) allows them to specify the use of that additional identity verification process for every transaction. If this is the case then why does section 12(1) of the Draft Determination not use the language of a valid request. Twilio notes that a valid request as defined in section 12(3) of the Draft Determination may still not be a reasonable request in the context of a customer and the services it is taking.
- 4.10 Or is section 12(2) of the Draft Determination intended to allow customers to specify a process that sits outside of the processes outlined earlier in the Draft dDetermination as opposed to an additional process. If that is the case then the earlier provisions need to be made subject to section 12.
- 4.11 Twilio suggests that the requirement for a provider to comply with the request of a customer must be deleted if the provider is going to be required to do so at no cost and particularly where there is no element of reasonableness applied to the request. The provisions should either be drafted in a way that allows a customer to make a reasonable request and the carriage service provider to accept but to charge the customer for the change or the provider must be allowed to reject the request. The cost of making a change for one customer for all their interactions with a provider in a particular environment will be considerable as it involves bespoke work.
- 4.12 Twilio also notes that sections 12(4) and 12(5) of the Draft Determination requires that if a carriage service provider suspects that a customer’s account has been the subject of fraudulent activity that the carriage service provider must no later than 24 hours of that suspicion arising contact the customer to offer the use of an additional identity verification process prior to undertaking any high risk customer interactions and if the customer accept the provider must use the process agreed with the customer. Twilio suggests that again this section is too prescriptive and again falls into the trap of imposing a one size fits all process. A carriage service provider should be able to discuss with a customer a solution that best meets the customers’ needs based on the suspected fraudulent activity.
- 4.13 Twilio suggests that the drafting of the provisions in section 12 of the Draft Determination suggests that ACMA thinks that adding in another authenticating factor is as simple as simply getting call centre staff to ask one more question. This is far from the truth and the ability of numerous customers to ask for one process for a call centre environment, one process for an online environment means that the carriage service provider faces the possibility of constant changes to processes and to customer training. The evidence for how this adds a benefit to customers is not spelt out and Twilio suggests that the whole of section 12 is disproportionate and not justified by any evidence produced by ACMA.
- 4.14 Finally, Twilio also has concerns about the record keeping requirement. Firstly it is not clear how these records of the application of MFA to every high risk customer transaction can be kept



in an easily retrievable form if these records can be kept at all and the requirement to provide them within five (5) working days is therefore extremely unreasonable. Twilio would urge ACMA to liaise further with industry on this requirement.