



Treasury Laws Amendment Bill 2024: Scams Prevention Framework

4 October 2024

Twilio welcomes the opportunity to comment on the Treasury Laws Amendment Bill 2024: Scams Prevention Framework exposure draft (the Bill) released by the Treasury. We appreciate the importance of scam prevention for all citizens and acknowledge the need for telecommunications providers to work together to tackle this challenging issue. We support the Government's focus on strong obligations on industry and encourage this in the context of maintaining a healthy telecommunications market for the benefit of all Australians.

ABOUT TWILIO AND STATEMENT OF INTEREST

Twilio is a global provider of cloud communications and customer engagement services to over 250,000 organisations globally. Twilio's products and services allow organisations of all sizes and across every industry – including non-profits, governments, and businesses – to embed communications capabilities in their web, desktop, and mobile applications, enabling them to communicate more efficiently and effectively with their customers.

Twilio has been operating in Australia since 2018, and powers the communications behind organisations in Australia across numerous sectors, including Westpac, Domino's Pizza, and Woolworths. We also work with not for profits such as Lifeline Australia and provide services to start-ups, small and medium businesses in every state and territory.

Twilio is committed to developing industry best practices and standards to maintain trust in the telecommunications ecosystem, and in particular to combat scam traffic. In the United States of America (US), for example, Twilio sits on the board of the Alliance of Telecommunications Industry Solutions, the Industry Traceback Group Executive Committee and Steering Committee, and co-chaired the Robocalling and Communication ID Spoofing Group which produced a comprehensive and coordinated view of all robocalling and spamming efforts across the industry and considered the need for further standards development.

In Australia, Twilio is an active member of Communications Alliance and is a voting member of a number of its working committees including those that have responsibility for the development of a number of industry codes that are relevant to the current consultation, namely: "Rights of Use of Numbers", "Integrated Public Number Database" and "Reducing Scam Calls and SMS". Twilio's involvement in these committees as a provider of software services and as a CSP as distinct from a carrier or mobile network operator means it has a unique and important perspective to offer.

Australia continues to be an important market for Twilio, and Twilio is continually improving its products and services for its 44,000 customers across Australia. Twilio is therefore keen to participate in policy discussions and developments, including on scam prevention, which will shape Australia's communications future.



TWILIO COMMENTS

Twilio is committed to supporting the Government's efforts to combat scam within the telecommunications network. Twilio also supports the submission of Communications Alliance and seeks to emphasise the following key points for consideration.

1. 'Prevent': a powerful tool in telecoms

Twilio is especially supportive of the 'prevent' principle which provides the first and most valuable opportunity to tackle scam. From Twilio's international experience in the telecommunications sector there are more effective and targeted opportunities to 'prevent' scam when engaging with the initiation of a communication, leading to actual scam reduction outcomes. In this context the use of authentication protocols such as the US' STIR/SHAKEN authentication framework, along with the operation of a 'Do-Not-Originate' list and 'know your customer' requirements is very effective.

Such protocols help ensure that traffic which fails to meet a number of initial standards doesn't make it onto the network (and can be legitimately stopped). In fact, use of authentication protocols to verify the legitimacy of caller information, effectively reducing the prevalence of spoofed calls has been an innovative solution that is now being adopted in many other jurisdictions^{1 2 3 4}. Since its adoption, there has been a decrease in fraudulent robocalls, as evidenced by consumer reports and US industry data⁵.

A valuable element of this system is that all providers are equal because each has responsibility for their own customers' traffic. This ensures the market is balanced and avoids creating a system where a few large stakeholders have disproportionate power over the full sector. We discuss this further under 'detect'.

2. 'Detect': limits of technical capabilities

Twilio is concerned that under the current drafting the principle 'detect' puts excessive power over traffic in the hands of a few dominant industry players, potentially without any scam reduction. This is because while there are many carriage service providers (CSPs) serving Australian businesses and consumers, by the time traffic reaches an individual around 95% of it goes through just three carriers^{6 7}. This means controls used by the carriers to 'detect' scam, which can be inaccurate, would impact almost all traffic on the telephone network.

Twilio supports the Communications Alliance's submission noting that the technology currently utilised within the telecommunications industry to 'detect' scam activity has limitations and is recognised as producing inaccurate findings. The inherent limitations in existing detection technology already result in significant volumes of false positives. This misidentification disrupts legitimate traffic and the service of the provider of that traffic as well. Smaller suppliers are disproportionately affected by these inaccuracies.

In this context Twilio would caution that the Bill should be restrained with the drafting of Subdivision D - SPF principle 3: detect. As currently drafted the Bill could provide a loophole

¹<https://www.gov.br/anatel/pt-br/assuntos/noticias/conselho-diretor-decide-ampliar-o-uso-do-codigo-0303-para-atividade-de-cobrancas-e-determinar-interlocucao-para-diminuir-falha-em-bases-cadastrais>

² <https://transnexus.com/blog/2024/shaken-in-france/>

³ <https://commsrisk.com/first-look-at-chaken-the-chinese-rival-to-stir-shaken-with-personal-avatars-and-video-id>

⁴ <https://commsrisk.com/brazil-to-begin-testing-end-to-end-validation-of-telemarketing-calls/>

⁵ <https://transnexus.com/blog/2024/shaken-statistics-april/>

⁶ <https://independentaustralia.net/business/business-display/big-news-revealed-for-australias-telco-industry,18436>

⁷ <https://www.statista.com/statistics/488511/australia-mobile-handset-services-market-share/>



for providers to decline to terminate traffic from other CSPs under the pretext of scam traffic. Legitimate traffic such as an emergency alert broadcast, a marketing campaign or appointment reminders could all trigger a pattern alert and be blocked unfairly. Potentially with disastrous outcomes. Therefore, patterns or use of a particular technology should not, on their own, be a reason to not terminate traffic.

Twilio urges the Treasury to consider the potential for market distortion and reduced competition through imprecise use of blunt tools particularly by larger providers, which would impact the services and operations of smaller providers as well as Australian end users.

3. Liability of Originating C/CSPs

To provide some management of the issues arising in point two Twilio encourages the Treasury to consider an amendment to Subdivision D - SPF principle 3 that would target the scope of this requirement. For the telecom industry this should ensure that only the CSP responsible for the origination of illegitimate traffic should be held liable for scam activity. In practice, telecommunications traffic often passes via multiple CSPs before terminating on an end user's device, for reasons of commercial agreements, software preference or traffic diversity needs.

Transit CSPs, which do not originate the traffic and therefore have no engagement with the customer (or scammer), have very limited ability to detect or validate the legitimacy of the traffic. Penalising transit CSPs for passing through traffic over which they have no control, or visibility would create both an unreasonable burden on the industry and lead to the unintended consequences noted at point 2.

By placing the liability appropriately with the CSP responsible for the origination of scam traffic the most effective anti-scam measures can be utilised, and unnecessary negative market and customer impacts can be avoided.

4. CSP Register for accountability

Twilio supports the calls in the Communication Alliance submission for the implementation of a register for all CSPs, as it would introduce clarity and accountability into the market. Currently there is no exhaustive list of CSPs operating in Australia. This makes it near impossible to ensure that all industry players are aware of and meeting their obligations.

By maintaining a comprehensive register of CSPs, it becomes easier to track the origination and flow of scam traffic, ensuring that only the responsible parties are held accountable. Furthermore, the establishment of a register would empower regulatory bodies to take effective enforcement actions and not need regulations that stifle innovation.

Without knowing where the industry begins and ends or who is operating in a market accountability and enforcement can't be achieved. In this context a CSP Register would be a valuable foundation for all anti-scam efforts.

Conclusion

Twilio supports the further arguments made in the submission from Communications Alliance. We encourage the Treasury to carefully weigh the points raised regarding market impacts, technical constraints, liability, and the need for supporting systems such as a CSP register. A balanced and thoughtful approach will be key to preventing scams effectively while maintaining a healthy telecommunications market for the benefit of all Australians.

Twilio appreciates the opportunity to contribute to this discussion and looks forward to further engagement with the Treasury.