

4th October 2024

Scams Taskforce
Market Conduct Division
Treasury
Langton Cres
Parkes ACT 2600

By email: scampolicy@treasury.gov.au

Pivotel welcomes the opportunity to comment on the Australian Treasury's draft SCAM Prevention Framework (SPF) exposure draft. This submission and associated commentary has necessarily been kept brief due to the limited time for review. Pivotel was a participant in the Treasury roundtable and briefing with the Assistant Treasurer.

The Pivotel group comprises Pivotel Group Pty Limited (Pivotel) and its wholly owned subsidiaries. Pivotel operates a mobile and satellite telecommunications network pursuant to a carrier licence issued by the Australian Communications and Media Authority in accordance with the *Telecommunications Act 1997* (Cth) (Telco Act).

Pivotel welcomes initiatives across the economy to combat scam. Pivotel is a participant in the working committee within Communications Alliance that prepared the Telco Anti-Scam Code and is actively involved in various forums and committees to combat SCAM including in establishing and advising the ACMA on the SenderID registry.

In addition to CA, Pivotel is an active member of the Australian Mobile Telecommunications Association (AMTA) and Commpete.

Pivotel is deeply committed to reducing scam and fulfilling its legal and regulatory obligations concerning the Reducing Scam Calls and SMS Code. We have made substantial investments in combating both scam calls and SMS to maintain the confidence of consumers and our clientele (both retail and wholesale). The effectiveness of our anti-scam measures is evidenced by the minimal scam traffic reported to us by national Mobile Network Operators (MNOs).

Our comprehensive scam prevention strategy encompasses:

1. **SecureSMS Initiative:** Over the past 4 years, Pivotel has developed an SMS authentication tool named "secureSMS". This technology has been showcased to various industry and government entities and is currently employed by several providers and companies.
2. **Reducing Scam Calls and SMS Code ("Scam Code"):** Pivotel played a key role in the Communications Alliance working group that formulated the latest version of the Scam Code.
3. **SMS SenderID Registry:** As one of four MNOs, Pivotel is actively testing and backing the implementation of the SMS SenderID Registry. We have engaged in consultations, presenting potential registry models and in-house developed proof-of-concept technology.
4. **Australian Financial Crimes Exchange (AFCX) Intel Loop:** Pivotel was an early adopter of the AFCX's "Intel Loop" initiative, which enables scam-targeted

organisations to report verified scam communications directly to MNOs. We are currently the sole MNO assisting in developing the system's application programming interface (API).

5. **National Anti-Scam Centre (NASC):** Pivotel has been actively involved in the NASC initiative, and was present at its inaugural meeting in 2023. We maintain representation in the Communication and Awareness Working Group under the NASC, collaborating with industry to educate Australians about scams and enhance scam reporting processes.
6. **Security and Fraud Alliance Forum:** Pivotel regularly participates in the Forum's quarterly discussions, presenting SMS scam mitigation models and proof-of-concepts to members.
7. **Proofpoint/Cloudmark Services Partnership:** Pivotel invests significantly in its collaboration with Cloudmark, a leader in threat protection, to continuously improve our threat detection and scam filtering capabilities.
8. **Scam Telecommunication Action Taskforce:** Pivotel has been an active Taskforce member since its inception. Notably, our presentation on sender ID message verification technology to the Attorney General's Department and Department of Home Affairs (supported by the Australian Cyber Security Centre) contributed to amendments in the Telecommunications Act 1997, enabling enhanced scam SMS screening.

Pivotel fully supports the Communications Alliance (CA) feedback on the draft SCAM Prevention Framework (SPF) which emphasises the need for a cohesive and flexible approach to combat scams across various sectors, including telecommunications, banking, and digital platforms.

In particular, Pivotel endorses the three key recommendations in the CA submission:

1. Move Specific Details to Sector Codes

The nature of the Telecoms industry structure is very different to other sectors. The detailed requirements proposed in the draft SPF are likely to create complexity and potentially unwarranted outcomes. Pivotel supports the view that detailed requirements should be transferred from primary legislation to sector-specific codes. This would allow for greater flexibility and easier enforcement by sector-specific regulators, such as the Australian Communications and Media Authority (ACMA) for telecommunications. Telecoms industry specifics, such as the technical and legal inability to scan content, as well as the sheer volume of traffic that traverses networks, provide some unique challenges and differences to the other sectors captured under the SPF.

The current broad application of the SPF may not suit all sectors due to their unique characteristics and operational differences.

2. Establish Safe Harbor from 'Quadruple Jeopardy'

The CA submission highlights concerns about telcos facing multiple layers of liability under the SPF, even when complying with sector-specific codes. Pivotel supports CA proposal to create a "safe harbour" provision that would protect telcos from enforcement by multiple regulators if they adhere to their sector's code. This would prevent unnecessary duplication of penalties and liabilities.

3. Accelerate Practical Measures Against Scams

Pivotel supports the swift implementation of the SMS Sender ID Registry.

Pivotel's views in relation to the Numbering Plan, is that the ACMA should clarify and confirm that the right to the use of numbers, sits with the end user, not the C/CSP, and provide clarity regarding the end-users legitimate use of numbers. In that context, illegitimate use of numbers, where the end user does not have the right to use, can be more confidently used as an indicator of scam.

Telecoms Industry SCAM Code

The telecommunications industry has been proactive in combating scams, evidenced by the development of industry codes enforced by ACMA since 2020. These efforts have resulted in a substantial decline in Voice and SMS scam volumes and scam-related financial losses as shown in the NASC report on Scams Activity 2023 which showed a reduction of 13% between 2022 and 2023.

The proposed SPF should build on this success by recognising sectoral differences and allowing for tailored regulatory approaches.

Risk of Over-Blocking

Pivotel is particularly concerned regarding overly prescriptive regulations that could lead to excessive blocking of communications including legitimate traffic, which has a real and immediate impact on consumers and downstream competition and choice. A balanced approach is necessary to ensure that compliance requirements do not incentivise carriers to adopt a heavy-handed approach.

Patterns or specific technologies alone should not justify blocking traffic. This approach is known to produce significant false positives, disrupting legitimate communications and disproportionately affecting smaller providers. Pivotel cautions against the potential for carriers to unjustly block traffic under the guise of scam prevention, as this could lead to blocking essential communications like emergency alerts or appointment reminders.

There are effective targeted industry approaches to SCAM reduction like in the US where they have adopted authentication protocols such as "Stir/Shaken", 'Do Not Originate' register and 'Know your Customer' requirements. These approaches are more effective at addressing scam at the source, as opposed to retrospective reporting and blocking where the scammers can adapt and modify their actions and stay ahead of scam prevention efforts.

Liability at the Source

Telecommunications traffic often passes through multiple CSPs before reaching the end user due to commercial agreements or technical needs. Transit CSPs, which merely pass along traffic without originating it, lack the ability to detect or verify its legitimacy. Penalising these transit CSPs would impose an unreasonable burden and could lead to unintended negative consequences.

By assigning liability to the CSP that originates scam traffic, more effective anti-scam measures can be implemented, avoiding unnecessary market disruptions and protecting legitimate communications. This approach ensures that accountability is placed where it can be most effectively managed, minimising impacts on smaller providers and end users.

Sector-Specific Regulation

By delegating detailed requirements to sector-specific regulations, the SPF can ensure that each sector's unique capabilities and limitations are considered.

Role of Telecommunications in Scam Prevention

Telecommunications play a crucial role in modern society, facilitating numerous services. However, they should not bear equal liability for scam-related damages across all sectors. Pivotel calls for limiting liability to instances of non-compliance with sector regulations, ensuring that telcos are held accountable only where appropriate.

Conclusion

Pivotel supports the need for a flexible, sector-specific approach within the SPF, to effectively combat scams while minimising unintended consequences. By adopting these recommendations, the framework can enhance its effectiveness across different industries, ultimately protecting consumers and businesses from scam-related fraud.