



4 October, 2024

Scams Taskforce
Market Conduct Division
Treasury
Langton Cres
Parkes ACT 2600
Email: scampolicy@treasury.gov.au

RE: Scams Prevention Framework – Submission on Exposure Draft Legislation

Transaction Network Services, Inc. (“TNS”) in conjunction with its subsidiary Transaction Network Services Australia Pty Ltd is pleased to submit these comments on the Scams Prevention Framework – Exposure Draft Legislation (“SPF”), dated September 2024.

About TNS

TNS is a global provider of infrastructure-as-a-service solutions for the communications, payments, and financial services industries. In the United States, TNS is a leader in anti-scam technologies for communications providers. TNS provides Call Guardian®, a machine learning analytics solution that uses over 1.5 billion cross carrier real-time call events per day and crowd-sourced data to create accurate and comprehensive call reputation profiles for purposes of blocking or labeling scam, nuisance, illegal or otherwise unwanted telephone calls. Call Guardian® is a leading platform in robocall identification accuracy and possesses capabilities for various types of carrier networks, numbers, and situations. It is used by four of the top seven U.S. carriers and five of the top seven wireless providers. In Australia, TNS is currently replacing the legacy Intelligent Network Services – Telephony Application Server (TAS) Inbound, Mobile Origin Location Indicator, TAS Number Portability, and Local Number Portability in the fixed and mobile networks of a major carrier.

TNS has provided services to the payments industry in Australia since the early 1990’s. Since 2016, TNS has been a member of the Australian Payments Clearing Association’s Community of Interest Network (COIN), a network connecting Australia’s largest banks for payments. In 2022, TNS was selected to provide AusPayNet’s next-generation network for COIN members. TNS migrated its first COIN member to the network in late 2023 and is in the process of migrating all COIN members during 2024. Accordingly, TNS has a wealth of experience partnering with Australian businesses and regulators to ensure the highest levels of network security and effectiveness.

TNS submission on the SPF

Based on this experience in Australia and the United States, TNS offers these suggestions for improving the Scams Prevention Framework.

Transaction Network Services, Inc.
10740 Parkridge Boulevard, Suite 100, Reston, VA 20191 USA
+1 703 453 8300 | tnsi.com
4872-0388-0172 v.2

1) Does the draft legislation effectively achieve the policy objectives set out in the document?

a. TNS Proposes Improvements to SPF Principle 2 (Prevent).

Defining measures that qualify as reasonable steps to prevent scams: verified identity solutions and discriminative AI

Although TNS acknowledges that the proposed legislation largely meets the stated policy goals, it also sees potential for further measures to safeguard consumers. Specifically, TNS suggests that SPF Principle 2 (Prevent) should define or state what qualifies as “reasonable steps” in either the legislation itself or the explanatory materials to include the requirement for businesses in all regulated sectors to use verified identity solutions for validating customers and network users. Alternatively, this should be included in any non-exhaustive guidance and/or sector specific Codes that will be developed as part of the SPF (see section 58BL).

Verified identity solutions are a relatively new innovation developed by TNS and competing service providers, and they are demonstrably effective in preventing scams by reducing the opportunities for scam artists to operate anonymously. Verified identity solutions generally include “know your customer” information collection and verification requirements, in addition to solutions to offer trusted validation when information is transmitted across communications networks. By incorporating these measures, the legislation can more significantly enhance consumer protection and trust in the digital ecosystem. TNS believes that such proactive steps are essential in the fight against fraud and scams and, accordingly, that including verified identity solutions in the definition of reasonable steps is warranted.

For instance, TNS offers Enterprise Authentication, Spoof Protection, and Enterprise Branded Calling (“EBC”) services to major brands in the US and is working on a proof of concept with a major carrier in Australia. These solutions work together as follows:

- Enterprise Authentication allows businesses to verify their calls through a pre-call API, ensuring only legitimate calls are displayed.
- Spoof Protection blocks unverified calls within the telecommunications network before they reach consumers.
- EBC, once these trusted interactions are established, provides consumers with information about the incoming call, such as the enterprise’s name, logo, and reason for the call, rather than just a phone number.

These solutions, along with similar offerings from other infrastructure-as-a-service providers, enhance trust in the network and business ecosystem, reducing the chances for scam artists to pose as trusted brands and exploit unsuspecting consumers. By implementing these services, businesses can significantly improve their communication security and consumer trust.

Requiring the adoption of verified identity solutions such as these as a “reasonable step” will provide certainty to regulated entities about what steps will meet this obligation, greatly enhancing security and reliability against scammers across the ecosystem and in all regulated sectors.

Moreover, it would directly support SPF Principle 2 by introducing additional identity verification requirements for new accounts, providing direct warnings to consumers and businesses about scam activity observed on or related to its service and steps that consumers can take to minimize the risk of harm.

Additionally, it facilitates proactively seeking out information from alternate sources on emerging scam activity to identify whether there are any particular vulnerabilities faced by the service, and further bolsters SPF Principle 2 by providing advanced tools and training to business staff on emerging scam activity to assist them in identifying and responding to evolving scams in real time.

Significantly, verified identity solutions shift the paradigm from a defensive, reactive stance to an offensive, proactive strategy to foster trust within the ecosystem. Governmental agencies that oversee corporate institutions and businesses (such as ACMA, ASIC, and ACCC) possess crucial information that can confirm whether businesses are registered and legitimate, and authorized to operate under public identities, including brands, logos, company names, and, by extension, telecommunications identities (phone numbers) and digital identities. This information can be utilized in conjunction with the verified identity solutions offered by TNS and other providers to authenticate and verify the entities engaging with the Australian public, similar to how Google collaborates with financial regulators to ensure that only registered financial organizations advertise on its platform in Australia. Regulators tasked with developing and enforcing the SPF must maintain consistency in their approach to administering and enforcing SPF Principle 2. By requiring the implementation of verified identity solutions up front, consumers will be better protected by the SPF and the ecosystem will benefit as a whole.

Verified identity solutions also are effective in reducing the financial loss of scams because they stop scams before they reach consumers, assist in the investigation of scams at all stages of the lifecycle, enable easier identification of the entities responsible, and support enforcement against scam artists. In addition, ecosystem members have at their disposal a growing number of AI-based tools for effective identification and control of scam activities. The principles-based obligations should encourage businesses to use advanced technology such as those offered by TNS and discussed above to fulfill the obligations identified.

Discriminative AI, i.e., technologies that classify and predict data, often serves as a helpful back-office tool for, among other things, the ability to target scams, particularly through illegal robocalls or SMS. This type of AI provides a means to identify abuses within an industry and ultimately aids the government in curbing illegal calls and texts. Discriminative AI serves as a consumer protection tool and should be employed where available.

Requiring verified identity solutions in conjunction with the use of discriminative AI and similar technologies would strengthen SPF Principle 2 by enhancing identity verification requirements, ensuring prompt and direct warnings are provided to consumers and businesses about scam activity, providing concrete steps that consumers can take to minimize risk, proactively developing intelligence from robust sources on emerging scam threats and vulnerabilities, and providing advanced training to staff to assist them in identifying and responding to scams quickly and effectively.

Accordingly, the use of verified identity solutions and discriminative AI technologies should be encouraged in furtherance of a business' obligation to take reasonable steps to prevent misuse of its services by scammers and also in furtherance of obligations to prevent and trace scams where scam intelligence is received. An effective way for the SPF to do so would be to include verified identity solutions as part of the definition of the reasonable steps businesses must take to prevent scams in either the legislation or code itself, or in the accompanying explanatory materials.

b. TNS Proposes Improvements to SPF Principles 3 (Detect) and 5 (Disrupt).

Use of robust data analytics

TNS wholeheartedly endorses the development and refinement of principles-based obligations and sector-specific codes to detect and disrupt scams, but suggests that the draft legislation could be enhanced by encouraging robust analytics solutions as a “reasonable step” for SPF Principles 3 (Detect) and 5 (Disrupt) and providing safe harbor from liability for providers based on the use of reasonable robust analytics.

Robust analytics refers to the use of advanced data analysis techniques and tools that can handle a wide variety of data inputs and conditions to effectively identify, detect, deter, and mitigate fraudulent activities. More specifically, it involves comprehensive data analysis, real-time monitoring, flexibility, generating and acting upon actionable intelligence, and predictive capabilities in support of detection and disruption operations. Robust analytics looks to all known aspects of a call or scam attempt and does not simply rely upon static features such as malformed numbers or invalid numbers in order to detect and disrupt scam attempts.

TNS has observed that scam artists are increasingly sophisticated in altering their tactics to evade detection and are now more proficient at bypassing traditional detection and disruption techniques, as well as manipulating industry standards to overcome protections. Robust analytics solutions afford businesses, TNS, and other service providers the ability to disclose sufficient information to its consumers to enable them to act in relation to the suspected scam and share that intelligence with regulators in real time, greatly improving the detection and disruption capabilities of the whole ecosystem. By mandating their use through the SPF legislation, consumers will benefit from enhanced protection, and businesses and regulators will be able to respond to emerging scam threats more quickly and accurately.

For example, as part of its robust analytics architecture, TNS publishes a comprehensive annual report on robocall activity in the U.S., complete with quarterly updates and highlights, detailing the evolving trends in the nature and origin of scam calls (<https://tnsi.com/resource/com/tns-2024-robocall-investigation-report-out-now-press-release/>). Furthermore, TNS features a “Robocall Scam of the Month” on its website, highlighting a significant scam and analyzing its tactics to alert consumers, businesses, and regulators in the ecosystem of the emerging threat (<https://tnsi.com/robocall-scam-of-the-month/>). These activities underscore the dynamic nature of scam tactics and the need for persistent vigilance. Robust analytics solutions empower consumers,

Transaction Network Services, Inc.

10740 Parkridge Boulevard, Suite 100, Reston, VA 20191 USA
+1 703 453 8300 | tnsi.com
4872-0388-0172 v.2

businesses, service providers such as TNS, and regulators to gather, analyze, and disclose sufficient information, enabling them to take action against suspected scams.

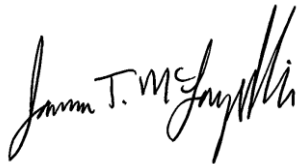
By sharing this intelligence with one another in real-time, these solutions significantly enhance whole-of-ecosystem approach to combatting scam taken by the SPF, making its inclusion as a “reasonable step” advisable. This approach not only improves the detection and disruption capabilities of the entire ecosystem but also ensures that preventive measures are effectively implemented and continuously assessed for their impact on protecting consumers.

Conclusion

In conclusion, incorporating verified identity solutions and robust analytics as mandatory steps within the already-admirable SPF framework will significantly bolster businesses’ ability to prevent, detect, and disrupt scams. This provides regulated entities with certainty about the steps they are expected to take and a comprehensive approach which ensures that both preventive and reactive measures are effectively integrated, enhancing the overall security and resilience of the ecosystem while better protecting consumers.

If you require further information, please do not hesitate to contact me or my Australian-based colleague, Bill Allen, Regional Sales Director- Transaction Network Services at wallen@tnsi.com.

Yours sincerely,

A handwritten signature in black ink, reading 'James T. McLaughlin'.

James T. McLaughlin
General Counsel and Secretary
Transaction Network Services, Inc.
+1 703 453 8534