29 January 2024

Scams Taskforce
Market Conduct and Digital Division
The Treasury
Langton Crescent
PARKES ACT 2600
Email: scamspolicy@treasury.gov.au

Re: Consultation on Mandatory Industry Codes on Scams

Transaction Network Services, Inc. ("TNS") in conjunction with its subsidiary Transaction Network Services Australia Pty Ltd is pleased to submit these comments on the Consultation Paper, "Scams – Mandatory Industry Codes," dated November 2023.

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.

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.

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

Overarching principles-based obligations (questions 15 and 16)

The proposed ecosystem-wide obligations should include obligations for businesses to employ verified identity solutions to validate customers and users of communications networks. Verified identity solutions should include "know your customer" information collection and verification requirements, in addition to solutions to offer trusted validation when information is transmitted across networks. Verified identity solutions are effective in reducing scams by reducing the opportunities for scam artists to operate anonymously. TNS provides Enterprise Authentication, Spoof Protection, and Enterprise Branded Calling ("EBC") services to major brands. With Enterprise Authentication, enterprises can authenticate their calls through a pre-call API so only verified legitimate calls are displayed. Spoof Protection blocks calls in the network without reaching the consumer for calls that are not verified. Once these trusted interactions with the enterprise are established, EBC provides information to consumers about the incoming call, such as the name and logo of the enterprise that is calling as well as the reason for the call, rather than merely a telephone number which the consumer may not recognize. These solutions provide trust in the network and reduce the ability of scam artists to masquerade as trusted brands in order to exploit unwary consumers.

Notably, verified identity solutions change the game from a defensive, reactionary approach to an offensive, proactive vehicle to create trust in the ecosystem. The governmental agencies that

regulate corporate institutions and businesses have valuable information that can be used to validate whether the businesses are registered and valid, and have the right to perform business under identities publicly, including brands, logos, companies names and, by extension, telecommunications identity (phone numbers) and digital identities. Use of this information can be used to validate and verify the instigators of engagement with the Australian public, in the same manner that Google has worked with financial regulators to implement policies to ensure that only registered financial organizations advertise on Google in Australia. Regulators that are responsible for enforcing future codes or standards need to be consistent in their approach to administer and enforce the Proposed Scams Code Framework.

Verified identity solutions also are effective in reducing the financial loss of scams because they assist in the investigation of scams, identification of the entities responsible, and enforcement against scam artists.

The use of verified identity solutions should be required 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 detect scams and to trace scams where scam intelligence is received. From a practical perspective, industry compliance teams may benefit from a prescriptive approach that their compliance, fraud and risk teams can use in the identification and control of scam activities.

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 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 and should be employed where available.

Information sharing and reporting requirements (question 28)

TNS agrees with the importance of information sharing arrangements within industries, across industries, and between the government and industry. Information sharing should be made available to service providers offering anti-scam solutions as well as to banks and other businesses serving customers. In the United States, TNS' Call Guardian® is fueled by information from a variety of sources, including government complaints and enforcement actions. To the extent that the NASC provides data-sharing to the ecosystem, it should include third-party anti-scam solutions providers in the sharing system. Accurate, up to date information is critical to correct conclusions and decisions. There should be effective mechanisms both for the push and pull of relevant scam information for approved organizations as:

- information can quickly become out of date; and
- the quality of how the information is inputted may vary and affect the accuracy.

This may extend to organizations outside of the telecommunications, banking, and digital communications platform industries discussed in the Consultation Paper. As an example, the Australian Fraud Crime Exchange database is presently limited to members and certain service providers, however other entities that operate in the Payments or Communications industries also may benefit from the information within it.

Information sharing should also be required in order to assist with the identification of scammers for enforcement purposes. U.S. carriers are required to participate in an industry "trace-back" process used to identify the origin of scam calls and to identify the carriers and customers responsible for such calls. Similar trace-back efforts across multiple industries could be facilitated by increased availability of and participation in such information sharing activities in Australia.

Sector-specific codes (questions 35 and 37)

TNS supports the creation and enhancement of sector-specific codes to combat scams and ensuring that the codes are transparent in their operation and contain appropriate appeal mechanisms. In addition to the obligations described in the Consultation Paper, TNS supports the use of robust analytics solutions to identify, block or otherwise remediate attempted scams. Robust analytics should look to all known aspects of a call or scam attempt, not simply use static features such as malformed numbers or invalid numbers. TNS' experience shows that scam artists are adept at changing their tactics to avoid scrutiny or to manipulate industry standards to defeat protections. TNS publishes a comprehensive annual report on robocall activity in the U.S., with quarterly updates and highlights, that outlines the changing trends in the nature and source of scam calls[1]. Additionally, TNS publicizes through its website the Robocall Scam of the Month[2] identifying a prominent scam and its tactics in order to warn consumers and the calling ecosystem of prominent threats. These activities underscore the constantly changing tactics of scam artists and the need for persistent vigilance. The use of robust analytics solutions can reduce the effectiveness of scam tactics and save consumers from financial harm from

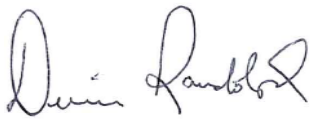
[1] https://tnsi.com/resource/com/tns-robocall-investigation-report/
[2] https://tnsi.com/robocall-scam-of-the-month/

scams. Each industry should explore the use of robust analytics solutions as part of their sector-specific codes.

TNS understands the need for consistent measures to be adaptable to new vulnerabilities when it relates to scams. The overarching regulatory framework and how technology can be used when businesses are implementing these regulatory obligations is key to the success of the proposed ecosystem-wide obligations.

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



Dennis Randolph
President – Communications Market
Transaction Network Services, Inc.
O +1 703 453 8534
M +1 571 309 8030