

TELSTRA GROUP LIMITED

ROBOCALLING MITIGATION PLAN

AS OF FEBRUARY 27 2026



ABOUT THIS PLAN

This plan details how Telstra Group Limited and its affiliates have implemented measures that can reasonably be expected to significantly reduce the origination of illegal robocalls on their networks. Each chapter of this plan sets out the methods and procedures that are implemented for Telstra Group Limited's consumer, enterprise, and wholesale voice offerings in Australia and by Telstra Group Limited's affiliates and subsidiaries in its international business (collectively, with Telstra Group Limited, "Telstra"):

Telstra Limited

Telstra UK Limited

Telstra International Limited

Telstra Telecommunications Private Limited

Telstra Singapore Pte Ltd.

Telstra Japan K.K

Telstra Services Korea Limited

Telstra Global Malaysia Sdn Bhd

Telstra Network Services NZ Limited

Telstra Philippines Inc.

Telstra (Thailand) Co., Limited

Telstra Services (Taiwan) Inc

This plan describes the specific reasonable steps Telstra Group Limited has taken to prevent new and renewing customers from originating or transiting illegal robocalls on Telstra Group Limited's network. This plan does not cover U.S. domestic service offerings provided by Telstra Incorporated, the U.S. subsidiary of Telstra. The policies and procedures implemented by Telstra Incorporated are filed in a separate Robocalling Mitigation Plan.

ABOUT TELSTRA

Telstra is Australia's oldest and largest telecommunications company, serving 8 million consumer customers and 19,000 enterprise customer entities throughout Australia and a further 6,000 enterprise customer entities globally. Although Telstra's heritage is proudly Australian, it has a longstanding international business. This includes providing telecommunications services to thousands of Australian and non-Australian businesses, government, carrier, and Over-the-Top ("OTT", i.e., streaming) and Voice-over-IP ("VoIP") customers, through establishments in 20 jurisdictions outside of Australia. These services are underpinned by an extensive network of affiliated carriers and licenses in Asia, Europe, and the Americas, as well as access to 2,000 points of presence in more than 200 countries.

© Telstra Limited (ABN 33 051 775 556) 2012. All rights reserved.

This work is copyright. Apart from any use as permitted under the Australia Copyright Act 1968, information contained within this publication cannot be used for any other purpose other than the purpose for which it was released. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the written permission of Telstra Limited. Any words mentioned herein that are known to be trademarks, whether registered or unregistered, have been capitalised or use initial capitals.

WHAT'S INSIDE

THE AUSTRALIAN REDUCING SCAM CALLS CODE	4
ANALYZING AND MONITORING NETWORK TRAFFIC	6
INVESTIGATING SUSPICIOUS CALLING	8
CUSTOMER ON-BOARDING AND KYC	10
CO-OPERATING IN TRACEBACK REQUESTS	13

Chapter 1

THE AUSTRALIAN REDUCING SCAM CALLS CODE

Telstra's Robocalling Mitigation Plan is based on its compliance with the Australian [C661:2022 Reducing Scam Calls and Scam SMS Code](#) ("the Code"). The Code sets out processes for identifying, tracing, blocking, and otherwise disrupting "Scam Calls" – defined by the Code as "any voice telephony call which has been generated for the purpose of dishonestly obtaining a benefit, or causing a loss, by deception or other means."

The process to disrupt Scam Calls, as required by the Code, is built on improved information sharing between Carriers/Carriage Service Providers¹ ("C/CSPs"), as well as improved information sharing between industry and relevant government agencies. It includes obligations on C/CSPs to adopt methods and procedures for:

1. analyzing and monitoring network traffic;
2. investigating suspicious calling; and
3. cooperating in traceback requests.

Telstra is required by law to comply with the Code, which is enforceable by the Australia Communications and Media Authority ("ACMA"). ACMA is the regulatory equivalent of the United States Federal Communications Commission ("FCC"). Telstra played a leading role in the development of the Code, to include Chairing the [Communications Alliance](#) working group that led to its development.

Under the Code, C/CSPs such as Telstra have several obligations including monitoring, tracing, and blocking Scam Calls. These include requirements for C/CSPs to:

- monitor for Scam Calls based on described characteristics;
- trace Scam Calls to their originating or transiting C/CSP;
- advise a C/CSP when it delivers Scam Calls;
- monitor for Scam Calls using the characteristics of Scam Calls set out in section 4.1 of the Code;
- block confirmed Scam Calls based on CLI that are found to be originating from, or transiting to, a C/CSP's network, as close to the source as possible;
- share information with C/CSPs about the origin and transit path of Scam Calls;
- advise an international operator to stop the delivery of Scam Calls into Australia from identified CLIs; and
- use all available contractual arrangements to secure the assistance of international operators in stopping Scam Calls into Australia.

The ACMA signed a Memorandum of Understanding ("[MOU](#)") with the FCC in May 2021 that seeks to enhance cooperation between Australia and United States regarding Scam Calls.² The MOU will foster the ability of the

¹ Carrier and Carriage Service Provider are defined by sections 7 and 87 (respectively) of the [Telecommunications Act 1997](#) (Cth).

² Memorandum of Understanding Between the United States Federal Communications Commission and the Australian Communications and Media Authority on Mutual Assistance in the Enforcement of Laws on certain unlawful communications, May 28, 2021 (available at: <https://docs.fcc.gov/public/attachments/DOC-372922A1.pdf>).

FCC and ACMA to work together to combat unlawful robocalls, unsolicited texts, and phone scams by exchanging information for the purpose of enforcing and securing compliance with anti-robocalling and spoofing laws.

Implementation of the Code has led to a reduction in reported phone scam of more than 50%.³ Telstra has blocked over 250 million Scam Calls.

The methods and procedures implemented by Telstra's international affiliates are also required to comply with local regulations to prevent robocalling and scam calls.

³ <https://www.accc.gov.au/speech/making-australia-a-harder-target-for-scammers-keynote-address>

Chapter 2

ANALYZING AND MONITORING NETWORK TRAFFIC

CODE REQUIREMENT (EXTRACT)

4.3 Monitoring for Scam Calls

4.3.1 C/CSPs must monitor their networks for Scam Calls based upon:

- (a) the characteristics in sections 4.1 and 4.2 noting that these characteristics are not intended to be exhaustive or restrictive in terms of monitoring that may occur; and
- (b) the CLI notified by other C/CSPs or from relevant government agencies which are associated with potential Scam Calls.

NOTE: Each C/CSP is responsible for determining how they monitor their networks to detect Scam Calls on their networks.

TELSTRA'S IMPLEMENTATION OF THE CODE IN AUSTRALIA

Telstra's primary tool for meeting the Scam Calls monitoring and blocking obligations defined in the Code is known as Number Barring and Treatment ("NUMBAT"). This tool provides Telstra with a data feed, filtering, and blocking functionality, which collectively work to protect its customers and consumers in the United States from Scam Calls. The NUMBAT tool also protects Telstra's network and calling products from fraudulent use and/or misuse by bad actors. Telstra uses [REDACTED] to analyse NUMBAT call detail records (CDRs) to identify scam calls (Wangiri and incoming calls with spoofed +61 & international CLI), while the NUMBAT tool performs the integrated voice recording treatment/blocking.

Data Feed

Call establishment signalling messages for calls arriving onto and leaving the Telstra network are fed via the NUMBAT platform.

Filtering

NUMBAT passes each call through its filtering and analysis programs using call setup information such as calling and called party numbers as well as other data. Calls that are list matched or meet programmed criteria for blocking are rejected. Blocklists are populated automatically via detection algorithms in real time or manually as needed.

Blocking

NUMBAT applies call rejection capabilities to calls identified as meeting the criteria for such treatment. For example, the NUMBAT tool automatically blocks the following call cases:

- Missing or Invalid Australian or International CLI, including North American Numbering Plan (NANP) numbers.
- Unallocated Australian CLI
- Use of Freecall or other Inbound numbers as CLI
- Unallocated Country Codes and Regions

- “Wangiri” calls (identified in real time, and updated every minute or less)⁴
- Spoofing

METHODS AND PROCEDURES IMPLEMENTED FOR INTERNATIONAL ENTERPRISE OFFERING AND INTERNATIONAL WHOLESALE OFFERINGS

The following process is in place for analysing and monitoring network traffic for International Enterprise and Wholesale offerings:

Data Feed

A call detail record for each voice call, including origination and termination numbers, country, customer, and supplier, is sent from the voice switching network to the voice management database.

Filtering

At the voice management database, each call detail record then passes through four filters. Each filter contains different algorithms to detect if the call is suspicious.

These algorithms have been developed over time, and continue to be refined based on Telstra’s experience and known characteristics of scam calling activities.

Blocking

If the alert identifies a Scam Call, then a call blocking protocol is implemented on the network. Depending on the scenario, blocking can be implemented on the originating or terminating number, on a wider numbering range or on the whole customer trunk, depending on the specific nature of the traffic. Telstra notifies its customers and suppliers when such blocking occurs.

⁴ In the “Wangiri” scam (also known as the “one-ring scam”), a scammer typically places a call and causes it to disconnect after a short ring time, usually less than 10 seconds, in order to induce the called party to call back and incur toll charges, of which the scammer gets a share. See Report and Order, Protecting Consumers from One-Ring Scams, 35 FCC Rcd 14236, FCC 20-171, ¶ 3 (Nov. 30, 2020).

Chapter 3

INVESTIGATING SUSPICIOUS CALLING

CODE REQUIREMENT (EXTRACT)

4.4 Exchanging information about alleged Scam Calls

- 4.4.1 If a C/CSP identifies a material issue of alleged Scam Calls in calls received from other C/CSPs, that C/CSP (the Notifying C/CSP) must provide details of the alleged Scam Calls to the Originating C/CSP or Transit C/CSP which delivered the alleged Scam Calls to it, for investigation as soon as practicable, via an agreed electronic means (with a copy to the ACMA).
- 4.4.2 Details of the alleged Scam Calls to be provided in a notification under clause 4.4.1 should be in the format set out in Appendix A and must include:
- (a) the date and time (with UTC offset) of the alleged Scam Calls;
 - (b) the CLI used for the alleged Scam Calls;
 - (c) the number of alleged Scam Calls identified in the relevant period; and
 - (d) further evidence if requested by the Originating C/CSP or Transit C/CSP (e.g. customer complaints, call characteristics, CDRs) to support the identified calls as being alleged Scam Calls rather than legitimate calls.
- 4.4.3 C/CSPs must accept and acknowledge, via agreed electronic means (with a copy to the ACMA), receipt of a notification under clause 4.4.1.
- 4.4.4 If the Notifying C/CSP provides the notification under clause 4.4.1 to a Transit C/CSP, the Transit C/CSP must, as soon as practicable, forward the details (with a copy to the ACMA) to the C/CSP from which they received those calls.
- 4.4.5 The process in clause 4.4.4 must be repeated by all Transit C/CSPs until the Originating C/CSP or International Operator is reached.

TELSTRA'S IMPLEMENTATION OF THE CODE IN AUSTRALIA

Telstra receives Scam Call complaint data from various sources, including:

- Regulator data on Scam Call complaints, received from the Australian Competition and Consumer Commission ("ACCC") and the ACMA;
- The Telstra Unwelcome Calls (UWC) Centre, which takes complaints from our customers about Scam Calls received, along with complaints relating to our customers' numbers being 'spoofed' by scammers; and
- Evidence of Scam Calls from the NUMBAT tool.

This complaint data is analyzed and compared to our high-volume call data for the relevant period. The traceback process is initiated where we identify a material number of calls suspected to be Scam Calls.

METHODS AND PROCEDURES IMPLEMENTED FOR INTERNATIONAL ENTERPRISE OFFERINGS

For Telstra's enterprise offerings, the process to investigate suspicious calling includes four key steps involving teams at Telstra and our suppliers to support the end-to-end investigation. These steps are as follows:

1. Receive request for investigation of suspicious calling
 - a. Telstra validates the request and initiates its investigation.
2. Investigate activity associated with suspicious calling
 - a. Depending on whether the request is at the customer or Telstra network level, Telstra voice network experts are engaged to conduct the investigation. If the investigation occurs at the customer level, Telstra works with the applicable customer, informing and assisting them with the investigation.
3. Remediation and mitigation steps (if required)
 - a. **Customer Level:** if investigations reveal suspicious activity at the customer level, Telstra will inform the end user customer of the steps required to mitigate the activity. For example, this may include blocking at the originating or terminating number or number range.
 - b. **Network Level:** if investigations reveal activity at the Telstra network level, Telstra will undertake the necessary steps to manage and mitigate this activity. [REDACTED]
4. Summarized outcome of investigation
 - a. Upon completion of either the customer or network blocking, Telstra documents its findings for future reference within its systems. If a customer was impacted, Telstra updates the customer on the mitigation steps that were undertaken.

METHODS AND PROCEDURES IMPLEMENTED FOR INTERNATIONAL WHOLESALE OFFERINGS

Investigating suspicious calling for International Wholesale offerings is managed by a dedicated team of Telstra professionals that provides business and after-hours support. Alerts are generated for all calls that fail on any one of the wholesale filters, as described in Chapter 2. These alerts are analysed by Telstra's voice destination management team to determine appropriate follow up actions.

Chapter 4

CUSTOMER ON-BOARDING AND KYC

CODE REQUIREMENT

NOTE: Although there are no KYC requirements in the Code, Telstra has processes in place to verify the identity of all Australian domestic customers. These processes are summarized below.

TELSTRA'S IMPLEMENTATION IN AUSTRALIA

Telstra has a policy to verify the identity, suitability, and risks involved with onboarding unestablished customers. The purpose of Telstra's KYC processes is to ensure that all potential customers are who they claim to be.

Individual customers

A **100 Points of ID check** is performed when an unestablished customer requests any of Telstra's services. The unestablished customer is required to provide one primary ID and two forms of secondary ID or two primary IDs that verify their identity. An unestablished customer is classified as a customer who has been with Telstra for less than six months.

Established customers (with more than six months of history with Telstra) are authenticated through established processes that validate the identity of the customer. This can be by the customer providing physical ID or providing identifying information that can be validated against their existing customer record with Telstra.

Company, Corporate and Government customers

For customers that have a business with an Australian Business Number (ABN) or Australian Company Number (ACN), partnerships, joint ventures, trusts, incorporated associations, and government entities, Telstra authenticates the customer or the customer's authorised contact in accordance with the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022*.

METHODS AND PROCEDURES IMPLEMENTED FOR INTERNATIONAL ENTERPRISE OFFERINGS

Telstra has policies and procedures in place for both new and existing customers to validate an organization's identity and validity. Established processes and policies ensure that our customers are utilizing Telstra's services for legitimate and legally compliant purposes. Telstra has implemented 3 areas of focus:

1. New Customer Onboarding

Customers that have not previously contracted any product or service from Telstra are considered 'New Customers'. These customers are required to provide the following information to verify their organization:

- Customer name;
- Customer contact (mobile number, landline number, email);
- Legal entity name the customer will contract with;
- Customer address; and
- Website.

Through the onboarding process, a customer is vetted against existing customers within our system to check whether there is a duplication of records (some customers utilize different entities in different regions)

[REDACTED]. Customers are also assessed on their credit performance through a third-party credit check process to validate their financial capability and assess their business legitimacy.

2. Existing Customer Re-Validation

Customers that have previously contracted or procured any product or service from Telstra are classified as 'Existing Customers'. An Existing Customer is subject to Telstra's New Customer Onboarding Process if it:

• [REDACTED]

Customers who fall into one of the two categories above undergo a credit check to validate the customer's financial viability over the previous year. The New Customer Onboarding Process is followed every time a customer signs a new order with Telstra. Finally, Customer accounts are managed on an ongoing basis to ensure the contacts are updated in our systems and our suppliers' systems.

3. Provisioning

When services are provisioned or decommissioned, there are three scenarios:

- Port In: the customer is required to submit a Letter of Authorization ("LOA") to authorize Telstra to port a number from another carrier to Telstra's U.S. supplier. This process ensures the request is a legitimate one and that the information supplied by the customer is accurate. In addition to the LOA, customers must provide certain prescribed information to support geolocation – this includes the end user's address (suite/unit number, building name, street number and name, city, state, zip code, and country). Without the customer's LOA and address information, Telstra will not trigger a port in request.
- Port Out: the customer is required to advise Telstra of the carrier to whom the existing number is being ported. Telstra will not authorize a port out request without customer confirmation to ensure the request is legitimate and that the customer is aware of and approves the action.
- New Provision: customers supplied with new DID numbers are provided with such numbers by Telstra. Customers must supply certain prescribed information for all their DIDs, including contact and address information (suite/unit number, building name, street number and name, city, state, zip code, and country). Telstra will not provision a number without this information.

Know Your Upstream Provider

Telstra has incorporated reasonable procedures designed to ensure that it knows its upstream providers. Among other things, Telstra exercises reasonable due diligence before it begins accepting traffic from its upstream providers including the collection of certain information that includes, but is not limited to, obtaining each upstream provider's physical business location, contact person(s), state or country of incorporation, and other relevant information. In addition, Telstra's contractual agreements with its upstream providers, include provisions that can be exercised to address instances of suspected unlawful robocall traffic. Finally, Telstra has operational measures in place whereby it continues to work closely with its upstream providers to identify, investigate, and mitigate, suspected unlawful robocall traffic.

METHODS AND PROCEDURES IMPLEMENTED FOR INTERNATIONAL WHOLESALE OFFERINGS

New Customer Onboarding

Customers of Telstra International Wholesale offerings are vetting via the following processes:

- Telstra's engages Dun & Bradstreet to perform customer vetting checks. These checks are focused on the financial health of the new customer. However, Telstra also leverages these reports to better identify disreputable customers.
- Industry Forums: Telstra actively collaborates in industry and fraud forums to share information about fraud cases with our partners. This information sharing highlights repeat offenders who generate scam calls, in addition to raising red flags about customers who we should be wary of doing business with. Examples of the forums in which Telstra participates are i3Forum, Global Leader's Forum and Global Settlements Carrier Group.

Telstra's International Wholesale offerings terminate calls to the United States using suppliers that are required to comply with U.S. regulations. Furthermore, Telstra screens U.S. calls which pass through our network using fraud

detection algorithms. This means that U.S. calls pass through two independent filters to block Scam Calls (the filter on the Telstra network, and the filter on our supplier's network).

Know Your Upstream Provider

The same processes as outlined on page 11 apply to the Telstra International Wholesale offerings.

Chapter 5

COOPERATING IN TRACEBACK REQUESTS

CODE REQUIREMENT (EXTRACT)

4.5 Tracing Scam Calls

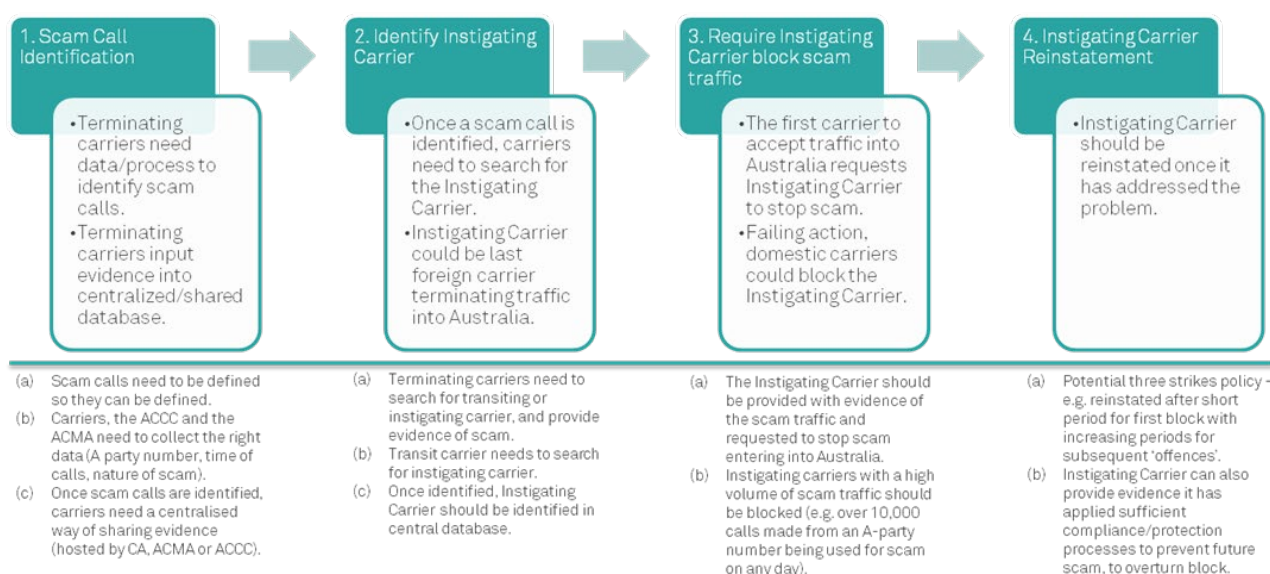
- 4.5.1 A C/CSP must have processes in place to trace the origin of alleged Scam Calls in accordance with section 4.4, whether the alleged Scam Calls originated on its own network or it was acting as a Transit C/CSP or Terminating C/CSP.
- 4.5.2 In accordance with the protection of communications provisions of the Act and the obligations at section 313(1) of the Act and section 474.17 of the Criminal Code Act 1995 (Cth), C/CSPs must cooperate with each other in the prevention, investigation and mitigation of Scam Calls which are using their Carriage Services.

TELSTRA'S IMPLEMENTATION OF THE CODE IN AUSTRALIA

Telstra has in place processes for tracing the origin of Scam Calls reported to us by C/CSPs, and for responding to traceback requests from the FCC's designated Traceback Consortium, which is currently USTelecom's Industry Traceback Group (the "Traceback Group").

Telstra responds to requests for traceback from C/CSPs and the Traceback Group by identifying the C/CSP that delivered the Scam Call to Telstra. Telstra then provides the traceback details to the requesting entity, which may include another C/CSP, the ACMA, or the Traceback Group. Telstra supports these traceback efforts so that the origin of the Scam Call can be identified. For requests made by the Traceback Group, Telstra's response is provided through the Traceback Group's portal.

SCAM CALL TRACEBACK PROCESS



METHODS AND PROCEDURES IMPLEMENTED FOR INTERNATIONAL ENTERPRISE OFFERINGS

Telstra takes the issue of unwanted and illegal robocalls seriously and is committed to ensuring that its network is not utilized for the origination of such calls. Subject to the legal limitations provided below, Telstra will therefore respond within 24 hours to all traceback requests from the FCC, the Traceback Consortium, and law enforcement agencies, consistent with the FCC's rules and regulations. Telstra has implemented processes and procedures to support traceback requests reported to us via the Traceback Group.

Telstra's traceback process is as follows:

1. Acceptance of traceback request from the Traceback Group
 - a. As a part of this task Telstra's assigned team will validate the Traceback Group's request and initiate the investigation.
2. Investigation of Traceback Request
 - a. Depending on the outcome on the traceback investigation feedback will result in either:
 - i. Closure of the investigation and documentation for internal purposes; or
 - ii. Remediation and mitigation if the patterns reflect origination on the Telstra network or from a Telstra end user.
 - b. In either case, Telstra will advise the Traceback Group of its findings.
3. Remediation and mitigation steps (if required)
 - a. End User Origination: If an end user is found to have been originating traffic suspected of being unlawful, Telstra will inform the end user customer who will be required to promptly investigate the traffic and report its findings back to Telstra. If the customer fails to take any remediation action, or if Telstra independently confirms that the traffic is illegal, then the customer's service traffic will be blocked from traversing to end users in the U.S. Telstra will also document its findings for internal tracking.
 - b. Originating at Network Level: if it is found that traffic is originating from our network, our team will block traffic from further traversing over the network and to end users in the U.S. All steps taken will be documented for internal tracking.
4. Feedback submitted via the Traceback Group portal
 - a. Telstra's team will submit required information through the Traceback Group portal.

Throughout this process, Telstra works closely with any U.S. suppliers.

METHODS AND PROCEDURES IMPLEMENTED FOR INTERNATIONAL WHOLESALE OFFERINGS

Telstra International Wholesale procedures for cooperating in traceback requests are as follows:

Notification

Telstra's wholesale service does not terminate calls directly to end users in the U.S. Instead, Telstra's wholesale service acts as a transit provider that sends voice traffic to other carriers that either further transits the traffic (*i.e.*, an intermediate provider), or terminates the traffic in the U.S (collectively a "Domestic Terminating or Transit Provider").

In instances where a Scam Call is detected, the Traceback Group will first contact the Domestic Terminating or Transit Carrier. The Domestic Terminating or Transit Carrier will respond to the Traceback Group that the calls were received from Telstra, at which point Telstra will provide the contact details for its upstream carrier.

Investigation

The Telstra Voice Account Manager will send details of the Scam Call provided by the Traceback Group to Telstra's Agile Network Operations Center ("ANOC"), with details about the time, date, and the originating and terminating telephone numbers.

ANOC will use these details to search our call records database using the Real Time Management System (RTMS). This search will provide details of the customer who sent the Scam Calls to Telstra.

Response

The Telstra Account Manager will respond to the Traceback Group with contact details of the customer who sent the calls to Telstra, so that the Traceback Group can continue down the call path to identify the origination of the Scam Calls.

Telstra's response will be entered into the Traceback Group portal by the Account Manager.

TRACEBACK CONTACT DETAILS

In accordance with the requirements for the FCC's Robocall Mitigation Database, Telstra provides the following information, including the name, title, department, business address, telephone number, and email address of the person within Telstra responsible for addressing robocall mitigation-related issues, to include traceback inquiries from the FCC, the Traceback Consortium, and law enforcement agencies:

Contact Name: Helene Valade-Nicolas
 Contact Title: Regional Manager – EMEA Voice
 Contact Street: The Crane Building, 22 Lavington Street
 Contact City: London
 Contact State and Zip Code: SE1 0NZ, United Kingdom
 Contact Telephone Number: +447970711764

Contact Email: InternationalCallTrace@team.telstra.com

OTHER LAWS IMPACTING ON TRACEBACK REQUESTS

Compliance with traceback requests from authorities outside Australia needs to take into account Telstra's obligations under the Telecommunications Act 1997 (Cth) and the Privacy Act 1988 (Cth).

Under the Telecommunications Act, carriers and CSPs are prohibited from using or disclosing a wide variety of information concerning communications, unless certain exceptions apply. One of those exceptions is where the information is required or authorised by or under law. Traceback requests are reviewed on a case by case basis to determine whether they meet this exception.

In addition, there are Australian Privacy Principles that govern among other disclosure of personal information, as defined under the Privacy Act, outside Australia. However, there are exceptions to the application of those principles where information is required by a law outside Australia or is necessary for the Australian entity to take appropriate action in relation to unlawful activity that relates to that entity's functions or activities.

Chapter 6

CERTIFICATIONS

1. Robocall Mitigation Plan

All calls Telstra originates or transits on its network is subject to this Robocall Mitigation Plan.

2. Filling in the Robocalling Mitigation Database

Telstra certifies its prior certification filed in the Robocall Mitigation Database has not been removed by Federal Communications Commission action, nor has it been prohibited from filling in the Robocall Mitigation Database pursuant to a law enforcement action.

3. Enforcement Actions and Investigations

At no time in the past two years, has Telstra been the subject of a formal action or investigation by the Federal Communications Commission, or other law enforcement or regulatory agency in the United States, which has resulted in findings of actual or suspected wrongdoing due to Telstra transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description. To the best of Telstra Group Limited's knowledge, no entity for which Telstra Group Limited shares common ownership, management, directors, or control been subject to any such action over the same time period.

4. STIR/SHAKEN Deployment

As a foreign voice service provider, Telstra has not deployed the STIR/SHAKEN standard since the ACMA has not mandated deployment of the standard. Given its status as a foreign voice service provider, Telstra also does not have an Operating Company Number (OCN).

5. Principals, affiliates, subsidiaries, and parent companies

Details about Telstra's principals, affiliates, subsidiaries, and parent companies can be found in the Telstra Annual Reports made available at <https://www.telstra.com.au/aboutus/investors/reports>.