

TELSTRA INCORPORATED

ROBOCALLING MITIGATION PLAN

FEBRUARY 23, 2024



ABOUT THIS PLAN

Consistent with the rules and regulations of the Federal Communications Commission (FCC), the following Robocall Mitigation Plan details how Telstra Incorporated (Telstra) prevents unlawful robocalls from originating from our enterprise voice product portfolio, which utilize numbers from the North American Number Plan (NANP). As detailed in this submission, Telstra has implemented a broad range of policies and procedures to ensure that illegal robocalls do not originate from its network. In addition to its robust existing policies and procedures, Telstra has also incorporated certain policies and procedures from external sources, including but not limited to: 1) the caller ID Authentication Best Practices outlined by the FCC in Public Notice DA 20-1526 ("FCC Best Practices", provided as Attachment A); and 2) the State Attorneys General (AG) Principles ("State AG Principles", provided as Attachment B). The chapters of this plan set out the methods and procedures for:

1. analyzing and monitoring network traffic;
2. investigating suspicious calling;
3. customer onboarding / Know Your Customer (KYC); and
4. cooperating in traceback requests.

Telstra is the U.S. subsidiary of Telstra Limited, Australia's oldest and largest telecommunications company, and consistent with the rules and regulations of the FCC, Telstra states that it:

1. is a voice service provider with a STIR/SHAKEN implementation obligation serving end-users, and has implemented STIR/SHAKEN; .
2. has not been prohibited from filling in the Robocalling Mitigation Database pursuant to a law enforcement action,
3. commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.
4. and/or any entity for which it shares common ownership, management, directors, or control, has not been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying 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 in the prior two years.

Telstra's interconnected VoIP product is called SIP Connect and is resold from [REDACTED]. As a result, Telstra relies on processes and technical capabilities built by [REDACTED] to comply with certain of our compliance obligations.

SIP Connect is a VoIP based unified communications service that facilitates multiple forms of voice, text, and data exchange through SIP trunking to fixed lines. There are two types of calls offered as part of a SIP Connect service:

- 1) inbound/incoming calls, where a customer receives calls on their assigned Direct Inward Dial (DID) number; and
- 2) outbound/outgoing calls: where a customer uses their assigned Direct Inward Dial (DID) number to make outgoing calls to international or local numbers.

Telstra Incorporated. Confidential. All rights reserved.

Information contained within this document cannot be used for any purpose other than the purpose for which it was released. No part of this document 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 Incorporated.

WHAT'S INSIDE

ANALYZING AND MONITORING NETWORK TRAFFIC	4
INVESTIGATING SUSIPICOUS CALLING	6
CUSTOMER ON-BOARDING AND KYC	7
COOPERATING IN TRACEBACK REQUESTS	10
FCC BEST PRACTICES	12
STATE ATTORNEYS GENERAL ANTI-ROBOCALLING PRINCIPLES	13

Chapter 1

ANALYZING AND MONITORING NETWORK TRAFFIC

APPLICABLE PRINCIPLES AND BEST PRACTICES

The FCC Best Practices recommend that providers implement caller ID authentication protocols, including the ongoing monitoring of subscriber traffic patterns, as part of their ongoing robocalling mitigation (FCC Best Practices, #5). In addition, the State AG Principles recommend that providers analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls (State AG Principles, #3).

TELSTRA'S IMPLEMENTATION

All lines served on Telstra's network are provisioned with a single telephone number, or a specific set of telephone numbers. These telephone numbers have been assigned only for the use on lines provisioned for that specified customer. All calls originated by any customer on Telstra's network must carry a Caller ID limited to one of the telephone numbers specifically assigned to that customer.

Telstra works closely with our U.S. supplier (REDACTED) to implement measures that can reasonably be expected to significantly reduce the origination of illegal robocalling from the Telstra network. Telstra has implemented processes and policies to analyze and monitor voice traffic traversing the Telstra network, including implementation of STIR/SHAKEN for U.S. traffic. This includes Telstra's 24/7 assurance team who manage and monitor voice traffic. Telstra has implemented four levels of assurance that focus on customer, call flows/traffic, the voice platform, and the network. Telstra works closely with its U.S. supplier (REDACTED) and we maintain direct communications when abnormalities are identified. The following provides an overview of the roles and responsibilities of Telstra's assurance teams in each of the four categories:

Function	Description
Customer	This team focuses on supporting our end users with their services. Customers can contact our team 24/7 with requests, such as investigation into high call volumes.
Call Flow/Traffic	This team provides 24/7 support to our Customer team and manages and monitors call flows and voice traffic. The team is comprised of technical experts who access and manage systems and Call Data Records ("CDRs") to analyze traffic.
Voice Platform	This team of technical experts focuses on the overall voice platform and supports our Customer and Call Flow/Traffic teams. Their role is to manage the platform and assist teams in implementing solutions at a platform level. The team is cross functional, and works closely with Telstra's Network team. Like the Call Flow/Traffic team, the Voice Platform team can access and analyze CDRs for investigation.
Network	Telstra's voice platform integrates with Telstra's MPLS network team, who utilize a variety of systems and tools to manage and monitor Telstra's voice services. Telstra's Network team supports the Call Flow/Traffic and Voice Platform team if there are any impacts to SIP Connect services. This team works closely with our voice team and operates 24/7.

CDRs

Telstra has the ability to analyze, monitor and identify calls originating from, or terminating to, the Telstra network based on their CDR data. (REDACTED)



Using STIR/SHAKEN, attestations are performed on outbound calls and verifications are completed on inbound calls. The validation result (Passed/Failed) is passed to customer in the INVITE field.

Customer Unique Identifiers

In addition to monitoring network traffic, Telstra assigns each of its customers a unique identifier. The unique identifiers are used by Telstra to facilitate more accurate analysis and monitoring of network traffic. These unique identifiers are assigned to all customers with SIP Connect services and users with multiple sites are assigned separate identifiers.

[REDACTED]

Identifiers are managed across Telstra's billing and engineering team to ensure alignment and accuracy for all customers.

Chapter 2

INVESTIGATING SUSPICIOUS CALLING

APPLICABLE PRINCIPLES AND BEST PRACTICES

The State AG Principles #4 address investigation of suspicious calls and calling patterns: “If a provider detects a pattern consistent with illegal robocalls, or if a provider otherwise has reason to suspect illegal robocalling or spoofing is taking place over its network, seek to identify the party that is using its network to originate, route, or terminate these calls and take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating commercial customer owns or is authorized to use the Caller ID number, determining whether the Caller ID name sent to a receiving party matches the customer’s corporate name, trademark, or d/b/a name, terminating the party’s ability to originate, route, or terminate calls on its network, and notifying law enforcement authorities” (State AG Principles, #4).

TELSTRA’S IMPLEMENTATION

For Telstra’s SIP Connect service, the process to investigate suspicious calling includes four key steps involving teams at Telstra and our U.S. supplier, [REDACTED] 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. For example, implementation blocks on the Session Border Control to minimize the suspicious activity at a platform level.
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.

Chapter 3

CUSTOMER ON-BOARDING AND KYC

APPLICABLE PRINCIPLES AND BEST PRACTICES

The FCC Best Practices address vetting procedures for voice service providers (FCC Best Practices, #1 - #4):

“1. Subscriber Vetting. Voice service providers should vet the identity of retail and wholesale subscribers, in conjunction with (i) approving an application for service; (ii) provisioning of network connectivity; (iii) entering into a contract agreement; or (iv) granting the right-to-use telephone number resources.

2. Telephone Number Validation. Originating voice service providers should confirm the end user or customer's right to use a telephone number.

3. Third-Party Validation Services. Originating voice service providers should use a third-party validation service when they cannot or choose not to independently perform telephone number validation in accordance with Best Practice #2.

4. International. Voice service providers that sell services to international call originators using North American Numbering Plan numbers should develop processes to validate that the calling party is authorized to use the telephone number or caller identity. Further, domestic gateway providers may wish to explore voluntary commercial arrangements with international providers that include terms and conditions that would give the domestic gateway provider the tools, information, and confidence to trust the validity of the calling identity.”

Similarly, the State AG Principles recommend that providers “confirm the identity of new commercial VoIP customers by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business” (State AG Principles, #5).

TELSTRA'S IMPLEMENTATION

Telstra has policies and procedures in place for both new and existing customers to validate an organization's identity and validity. The FCC's rules and regulations also require all voice service providers accepting traffic from an upstream provider to take steps to “know” that immediate upstream provider. Telstra's established processes and policies are designed to ensure that our customers are utilizing Telstra's services for legitimate and legally compliant purposes. Telstra has implemented 4 areas of focus:

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) and to verify that the customer is not an organization listed on our 'Exclusion List'. Telstra's Exclusion List is reviewed monthly and managed by our finance team to assess financial risk. The Exclusion List provides Telstra with additional internal information about the potential customer, whether it be from Telstra communicating directly with the

customer and/or from a financial perspective. 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.

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:

- is listed on our Exclusion List; or
- has not ordered any service or product from Telstra in the past 12 months.

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.

Provisioning

When SIP Connect 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 (REDACTED). 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 that are supplied with new Direct Inward Dial (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. The information is reported to our supplier (REDACTED) to support geolocation of the user in an emergency.

Contractual Arrangements

Telstra has also implemented contractual terms that can reasonably be expected to mitigate the origination of illegal robocall traffic from its network. All customers that sign up for a Telstra SIP Connect service will be required to agree to Telstra's terms and conditions ("Telstra Terms and Conditions"). The standard Telstra Terms and Conditions include the following provisions:

- **Telstra Contractually Requires Compliance with All Federal and State Laws.** The Telstra Terms and Conditions affirmatively obligate end users to comply with all applicable laws and regulations and requirements of any governmental body. Moreover, the Telstra Terms and Conditions expressly require compliance with the Telephone Consumer Protection Act, the Telemarketing Sales Rule, as well as the rules and regulations of the FCC.
- **Telstra Can Terminate Customers for Originating Illegal Robocalls.** The Telstra Terms and Conditions also permit Telstra to terminate any customer and discontinue their service if it is determined they are using the service in an unlawful manner. Telstra contractually retains the right to "immediately" terminate a customer in instances where Telstra determines in its "sole discretion" that the service is being used in an unlawful manner.
- **Telstra Mandates Customer Cooperation with Traceback Requests.** The Telstra Terms and Conditions also expressly require end user customers to cooperate with Telstra, as necessary, to support traceback inquiries. For example, customers of the SIP Connect service are expressly obligated to respond to traceback requests in a prompt manner, and to identify the customer or end user responsible for originating such traffic. These contractual provisions support Telstra's Traceback Request process as detailed below.

Know Your Upstream Provider

Based on the design of its voice network, Telstra's only upstream provider is (REDACTED). Telstra has various reasonable and effective measures in place with (REDACTED) to mitigate unlawful robocalls. Among other things, Telstra exercised reasonable due diligence before it began accepting traffic from (REDACTED) including the collection of certain information that includes, but is not limited to, obtaining Lumen's physical business location, contact person(s), state or country of incorporation, and federal tax ID. In addition, the contractual agreements between (REDACTED) and Telstra, 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 (REDACTED) to identify,

investigate, and mitigate, suspected unlawful robocall traffic (See e.g., Chapter 1, p. 4 (Analyzing And Monitoring Network Traffic), Chapter 1, p. 6 (Investigating Suspicious Calling)).

Chapter 4

COOPERATING IN TRACEBACK REQUESTS

APPLICABLE PRINCIPLES AND BEST PRACTICES

The State AG Principles detail the traceback practices that providers should implement (State AG Principles, #6 and #7):

“Principle #6. Require Traceback Cooperation in Contracts. For all new and renegotiated contracts governing the transport of voice calls, use best efforts to require cooperation in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered its network or by identifying its own customer if the call originated in its network.

Principle #7. Cooperate in Traceback Investigations. To allow for timely and comprehensive law enforcement efforts against illegal robocallers, dedicate sufficient resources to provide prompt and complete responses to traceback requests from law enforcement and from USTelecom’s Industry Traceback Group. Identify a single point of contact in charge of responding to these traceback requests and respond to traceback requests as soon as possible.”

TELSTRA’S IMPLEMENTATION

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. Telstra will therefore respond to all traceback requests from the Commission, the FCC’s designated Traceback Consortium, which is currently USTelecom’s Industry Traceback Group (the “Traceback Group”), and law enforcement agencies, within 24 hours, 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 as it relates to the Traceback Group 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 updated 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 instance, 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. Upon completion of all above steps Telstra's team will submit the required information through the Traceback Group portal.

Throughout this process, Telstra will work closely with our U.S. supplier ([REDACTED])

In accordance with the requirements for the FCC's Robocall Mitigation Database, Telstra has provided the name, title, department, business address, telephone number, and email address of the contact within Telstra responsible for addressing robocall mitigation-related issues, to include traceback inquiries from the FCC, the Traceback Group, and law enforcement agencies.

Contact Name: Helene Valade-Nicolas
Contact Title: Acting Regional Manager – EMEAA Voice
Contact Street: 2nd Floor, Blue Fin Building, 110 Southwark Street
Contact City: London
Contact State and Zip Code: SE1 0TA , United Kingdom
Contact Telephone Number: +447970711764

Contact Email: **InternationalCallTrace@team.telstra.com**

Attachment A

FCC BEST PRACTICES

Providers of voice service may use the following best practices as part of the implementation of effective call authentication frameworks to ensure the calling party is accurately identified:

1. **Subscriber Vetting.** Voice service providers should vet the identity of retail and wholesale subscribers, in conjunction with (i) approving an application for service; (ii) provisioning of network connectivity; (iii) entering into a contract agreement; or (iv) granting the right-to-use telephone number resources.
2. **Telephone Number Validation.** Originating voice service providers should confirm the end user or customer's right to use a telephone number.
3. **Third-Party Validation Services.** Originating voice service providers should use a third-party validation service when they cannot or choose not to independently perform telephone number validation in accordance with Best Practice #2.
4. **International.** Voice service providers that sell services to international call originators using North American Numbering Plan numbers should develop processes to validate that the calling party is authorized to use the telephone number or caller identity. Further, domestic gateway providers may wish to explore voluntary commercial arrangements with international providers that include terms and conditions that would give the domestic gateway provider the tools, information, and confidence to trust the validity of the calling identity.
5. **Ongoing Robocall Mitigation.** Voice service providers, whether IP- or non-IP-based, should have ongoing robocall mitigation programs in addition to implementing caller ID authentication protocols. The elements of such programs may vary depending on the nature of the voice service provider's business but may include ongoing monitoring of subscriber traffic patterns to identify behaviors that are consistent with illegal robocalling. Voice service providers may, after further investigation, take appropriate action to address such behaviors.

Attachment B

STATE ATTORNEYS GENERAL ANTI-ROBOCALLING PRINCIPLES

Principle #1. Offer Free Call Blocking and Labeling. For smartphone mobile and VoIP residential customers, make available free, easy-to-use call blocking and labeling tools and regularly engage in easily understandable outreach efforts to notify them about these tools. For all types of customers, implement network-level call blocking at no charge. Use best efforts to ensure that all tools offered safeguard customers' personal, proprietary, and location information.

Principle #2. Implement STIR/SHAKEN. Implement STIR/SHAKEN call authentication.

Principle #3. Analyze and Monitor Network Traffic. Analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls.

Principle #4. Investigate Suspicious Calls and Calling Patterns. If a provider detects a pattern consistent with illegal robocalls, or if a provider otherwise has reason to suspect illegal robocalling or spoofing is taking place over its network, seek to identify the party that is using its network to originate, route, or terminate these calls and take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating commercial customer owns or is authorized to use the Caller ID number, determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name, terminating the party's ability to originate, route, or terminate calls on its network, and notifying law enforcement authorities.

Principle #5. Confirm the Identity of Commercial Customers. Confirm the identity of new commercial VoIP customers by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business.

Principle #6. Require Traceback Cooperation in Contracts. For all new and renegotiated contracts governing the transport of voice calls, use best efforts to require cooperation in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered its network or by identifying its own customer if the call originated in its network.

Principle #7. Cooperate in Traceback Investigations. To allow for timely and comprehensive law enforcement efforts against illegal robocallers, dedicate sufficient resources to provide prompt and complete responses to traceback requests from law enforcement and from USTelecom's Industry Traceback Group. Identify a single point of contact in charge of responding to these traceback requests, and respond to traceback requests as soon as possible.

Principle #8. Communicate with State Attorneys General. Communicate and cooperate with state Attorneys General about recognized scams and trends in illegal robocalling. Due to the ever-changing nature of technology, update the state Attorneys General about potential additional solutions for combatting illegal robocalls.