

TG TELECO LLC
Robocall Mitigation Program
V.2 February 2025

STIR/SHAKEN Implementation

TG TELECOM, Inc. (“TG TELECOM” or “Company”) is an innovative global service provider providing secure, scalable solutions to the commercial and carrier market. TG TELECOM’s network solutions help customers control, scale and add value to their business through the use of innovative, cloud-based software platforms and next generation network services. TG TELECOM has fully implemented STIR/SHAKEN and on October 15, 2021 submitted its certification that all voice traffic originating on its network is authenticated with STIR/SHAKEN consistent with 47 C.F.R. §64.6301(a). Depending on the services being provided, TG TELECOM may serve as a Voice Service Provider, Gateway Provider, and/or Non-Gateway Intermediate Provider. As such, TG TELECOM submits this Robocall Mitigation Program (“RMP”) and certification into the Robocall Mitigation Database. This RMP includes the obligations outlined in the Commission’s recent release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (rel. March 17, 2023).

ROBOCALL MITIGATION

Background

The FCC Order requires that a RMP include the following affirmative obligations for voice service providers:

- Outline reasonable steps voice service providers have taken to avoid originating illegal robocall traffic;
- Commitment to respond 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;
- Know Your Customer procedures;
- Describe any call analytics system used to identify and block illegal traffic

Traceback

TG TELECOM is committed to ensuring its network is not utilized for the origination or terminating of illegal robocalls. TG TELECOM commits to responding fully and within twenty-four (24) hours to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium (“ITG”), and to cooperating with such entities in investigating and stopping any illegal

robocallers that attempt to use its service to originate calls. TG TELECOM is also actively involved in the ITG Traceback Group, and fully complies with the ITG Policies and Procedures.

TG TELECOM utilizes multiple reports that are built into their systems that will display calls related to the DNO and DNC lists statistically by customer. The results of this analysis may result in tickets being opened to the customer. In extreme cases the Company may suspend the customer's ability to transit traffic across the network until the issue can be thoroughly investigated and resolved directly with the customer.

The following describes the procedures TG TELECOM adheres to when conducting the investigations and to determine if the calls are actually illegal robocalls:

TG TELECOM has a multi-step approach designed to efficiently and effectively identify, analyze, and mitigate suspected illegal robocalls. This process leverages various tools and criteria to ensure compliance with legal standards and protect consumers from fraudulent and unwanted calls. This includes statistical analysis, velocity analysis and other computational methods for detection and mitigation of illegal robocalls:

Receipt of Traceback Request

- NOTIFICATION: TG TELECOM receives a traceback request from the ITG, FCC, or law enforcement. This notification usually provides details about the suspected illegal call(s), including timestamps, originating numbers, and destination numbers.
- ACKNOWLEDGEMENT: TG TELECOM acknowledges receipt of the request and may provide an initial estimate of the investigation timeline.
- REPORTING: TG TELECOM will report back to the ITG or other requesting entity within 24 hours.

TG TELECOM provides the following name, title, email address of the individuals within TG TELECOM that handles robocall mitigation-related issues as well as responding to traceback requests from the FCC, ITG, and law enforcement agencies:

Traceback Contact Information

[Call Blocking/Analytics for Monitoring Traffic:](#)

The Company has implemented its own call analytics to identify unlawful traffic that may originate on its network. These call analytics aid to identify behaviors that are consistent with illegal robocalling. TG TELECOM analyzes and monitors the traffic that originates on, terminates to, or

routes through TG TELECOM's voice network. If the Company identifies such calling patterns, it will take appropriate action to address the situation, including blocking such calls. As part of its analysis and monitoring procedures, the Company can utilize a real-time lookup system to detect where the calling number is invalid, unallocated, or on a Do Not Originate ("DNO"). If TG TELECOM's system detects any of these issues, a call will be released and a report is generated that provides the relevant details presented. TG TELECOM will then work with the originating customer to further investigate the issue and bring it to conclusion. TG TELECOM also monitors the Robocall Mitigation Database to verify all traffic is from a carrier that has registered in the database.

Pursuant to 47 C.F.R. §64.1200(n)(4) and its January 16, 2023 effective date, when serving as a Gateway Provider for voice traffic that is routing through its network, TG TELECOM takes reasonable steps discussed above to ensure that any Foreign Voice Service Provider or foreign Intermediate Provider from which TG TELECOM directly receives traffic is not using TG TELECOM to carry or process a high volume of illegal traffic onto the US network.

Know Your Customer Protocols

TG TELECOM has implemented affirmative, effective measures to prevent new & renewing customers from using its network to originate illegal robocalls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal calls. The Company has implemented Know Your Customer ("KYC") protocols when onboarding new or renewing customers. TG TELECOM will not provide service if a new customer's identification cannot be verified. These protocols include, but are not limited to the following:

- Initial Contact: When a new commercial/wholesale customer applies for a service they are required to provide personal identification information. This typically includes full legal name of the company (and its parent company if applicable), state or county of incorporation, physical address of its operations, billing name and address, and customer contact name and telephone number, federal tax ID and nature of customer's business. If the company is a Voice Service Provider, Foreign Voice Service Provider, intermediate Provider, and/or Gateway Provider, TG TELECOM will confirm that the company is listed in the FCC's RMD and has not been delisted pursuant to an enforcement action before accepting traffic from such entities.
- Document Verification: The customer must submit copies of official documents for verification. Examples include a government-issued ID card, passport, driver's license, utility bills for address verification, and other relevant personal or corporate documents.
- Know Your Traffic: Based on information provided, additional traffic information may be requested of the customer documenting the origins and compliance of the traffic
- Risk Profiling: Based on information provided, the carrier assesses the risk level of the customer. Factors such as the customer's location, the services they are requesting, and their financial considerations can influence their risk profile.

- Monitoring and Reporting: High-risk customers may be subject to more stringent monitoring of their account activities. This may include but are not limited to periodic reviews with the customer of their traffic, risk profile and analysis.
- Transaction Monitoring: TG TELECOM monitor transactions and use patterns for any unusual or suspicious activity that deviates from the customer's typical behavior.
- Update Customer Information: TG TELECOM periodically request customers to update their information to keep records current. This process may involve re-verifying identity documents and conducting additional checks for high-risk customers.
- Compliance Checks: Regular checks against local and international watchlists, including those for sanctioned individuals and entities, to ensure compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations.

Validating Customer's Right to Use Telephone Numbers:

TG TELECOM has procedures in place to authenticate the proper use of telephone numbers associated with calls routed over its network. TG TELECOM assigns customers numbers that are registered to TG TELECOM, and are assigned from the Company's direct inventory of numbers secured directly from NANPA. TG TELECOM does not provide a service where a customer can bring its own phone number from a 3rd party network, but must port-in a number to TG TELECOM to gain service. TG TELECOM also has processes in place to ensure that customer telephone number assignment is properly inventoried and tracked.

Accepting Traffic From Other Providers

Domestic Voice Service Providers

In accordance with 47 C.F.R § 64.6305(e)(1), TG TELECOM only accepts calls directly from a domestic Voice Service Provider only if that Voice Service Provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.

Foreign Voice Service Providers/Foreign Intermediate Providers

In accordance with 47 C.F.R § 64.6305(e)(2), beginning April 11, 2023, TG TELECOM only accept calls directly from a Foreign Voice Service Provider or Foreign Intermediate Provider that uses North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States, only if that foreign provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.

Gateway Providers

In accordance with 47 C.F.R § 64.6305(e)(3), beginning April 11, 2023, TG TELECOM only accepts calls directly from a Gateway Provider only if that Gateway Provider's filing (a) appears in the RMD, (b) shows that the Gateway Provider has affirmatively submitted the filing, and (c) has not been de-listed pursuant to an enforcement action.

Despite the above paragraphs in this Section, in accordance with 47 C.F.R § 64.6305(e)(4) and 47 C.F.R. § 64.1200(k)(5)-(6), TG TELECOM does not block a voice call if the call is an emergency call placed to 911. In addition, TG TELECOM makes all reasonable efforts to ensure that it does not block any calls from public safety answering points and government emergency numbers.

Authenticating Voice Traffic

In accordance with 47 C.F.R § 64.6301(a), when operating as a Voice Service Provider, TG TELECOM, to the extent technically feasible, will authenticate and verify originator identification information for all SIP calls that transit its own network, as well as all SIP calls it originates and will exchange with another Voice Service Provider or Intermediate Provider. TG TELECOM will, to the extent feasible, transmit that call with authenticated caller identification information to the next Voice Service Provider or Intermediate Provider in the call path. TG TELECOM will also verify originating identification information for all SIP calls it receives from another Voice Service Provider or Intermediate Provider which it will terminate and for which the caller identification information has been authenticated.

Pursuant to 47 C.F.R. §64.6302(b) and (c), when operating as a Gateway or Intermediate Provider, TG TELECOM will, authenticate caller identification information for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the Caller ID field and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call.

Acceptable Use Policy

The Company has specific Terms and Conditions within the customer contract to aid its customers to understand the intended and permissible uses of our service, and to prevent exploitation, fraud, and abuse of our calling plans and features. These terms include providing the Company the ability to pause, suspend, or otherwise terminate a customer found to be participating in any illegal activity, including generation of illegal robocalls.

CONCLUSION

The Company submits this Robocall Mitigation Program consistent with FCC Regulations, 47 C.F.R. §64.6305 (a)(1) & (d)(5). TG TELECOM will update its submission in the RMD within 10 business days of any change to the applicable information it must provide in the RMD, including its RMP.