
J&J Telecommunications, Inc.

Robocall Mitigation Plan

Background

Under the authority Congress granted the Federal Communications Commission (“FCC” or “Commission”) in the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, the Commission has adopted rules requiring voice service providers, like J&J Telecommunications, Inc. (“J&J”), to implement STIR/SHAKEN caller ID authentication technology in the Internet Protocol (IP) portions of their networks. 47 CFR § 64.6301.

The FCC requires that all voice service providers certify, by February 26th, 2024 in the Commission’s Robocall Mitigation Database whether they have implemented STIR/SHAKEN and that they have documented and instituted a robocall- mitigation plan to help combat the origination of illegal robocalls on their networks. The Commission has explained that a robocall-mitigation program is sufficient if the detailed practices in the plan can “reasonably be expected to significantly reduce the origination of illegal robocalls” and the voice service provider complies with the practices it describes in its filings.

J&J is dedicated to stopping illegal calls from originating on its network and undertaking commercially reasonable efforts to monitor the calls coming into its network, consistent with FCC regulations and its “Best Practices” guidance.

This document outlines J&J’s Robocall Mitigation plan.

J&J’s “Know Your Customer” Standards

J&J is a hosted voice service provider that focuses its business and operations on the small to medium size customer segments of the voice services communications market. As part of its customer-onboarding process, J&J undertakes various commercially reasonable precautions to verify a given prospective customer’s identity and relevant business practices before entering into a formal written agreement with that customer. All prospective customers must complete a questionnaire which provides J&J with detailed information about the customer. This questionnaire solicits vital information, such as:

1. Name of contact person responsible for account, and the name of the person responsible for payment;
2. Customer’s state or country of incorporation;
3. Description of the nature of the customer’s business;
4. The customer’s federal taxpayer identification number or equivalent;
5. Customer’s billing address and all physical addresses at which customer conducts business and from where calls may be originating.
6. J&J only provides service to direct customers. J&J is not a wholesale provider of voice services and does not provide service to resellers.
7. In response to our December 6th, 2024 Failure to Comply notification, we submit the following addition. As a micro-provider, we do not use any third-party analytics vendor and therefore have no vendor to name.

J&J's Acceptable Use Policy (AUP)

As part of its customer-onboarding process, J&J's customers will contractually agree to various terms and conditions, including a commitment to comply with J&J's Terms of Use. Among other things, these Terms prohibit:

- Using the Services to engage in any activities that are illegal, abusive, false, fraudulent, deceptive or misleading, or any activity that exploits, harms, or threatens to harm children.
- Engaging in any unsolicited advertising, marketing, or other unlawful activities using the Services that violate laws applicable to advertising, electronic communications, and telemarketing, including, but not limited to, Section 5 of the FTC Act (15 U.S.C. § 45), the CAN-SPAM Act (15 U.S.C. §§ 7701-7713), the Telemarketing Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108), the Federal Trade Commission Telemarketing Sales Rule (16 C.F.R. § 310 et seq.), the Telephone Consumer Protection Act (47 U.S.C. §§ 227), the Federal Communications Commission regulations (47 C.F.R. 64.1200 et seq.) and orders implementing the Telephone Consumer Protection Act, and all federal and state Do Not Call and calling-time restriction laws and regulations.
- Using J&J Telecommunications, Inc.'s Services in any way that fails to conform to any applicable industry guidelines and standards, including, without limitation, the CTIA Messaging Principles and Best Practices, Short Code Registry Best Practices, and Short Code Monitoring Handbook.
- Creating a false identity, forged email address or header, phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or phone call, including failing to comply with the Truth in Caller ID Act.

J&J's contracts with its customers will stipulate that it is authorized to suspend and/or terminate all Services in the event of an AUP violation.

Telephone Number Authorization and STIR-SHAKEN Capabilities

J&J is a small voice service provider, serving fewer than 100,000 voice service subscriber lines and therefore qualified for an extension until June 30, 2023 of STIR SHAKEN Implementation under 47 C.F.R. §64.6304(a)

J&J has now completed implementation of this requirement with the following capabilities:

- Complete STIR/SHAKEN implementation with all outbound VoIP calls signed with 'A' level attestation.
- Complete STIR/SHAKEN implementation with all inbound VoIP calls inspected for STIR/SHAKEN attestation.
- Enforceable outbound call limitations for all customers for mitigation of rapid-fire robocalls including instant notification and alert generation for any instance when call limits are reached.
- Enforceable outbound call limitations for entire customer base enterprise for mitigation of rapid robocalls including instant logging and alert generation for any instance of call limit being reached.
- Enforceable inbound call limitations for all customers for mitigation of rapid-fire robocalls including instant notification and alert generation for any instance when call limits are reached..
- Enforceable inbound call limitations for entire customer base enterprise for mitigation of rapid robocalls including instant logging and alert generation for any instance of call limit being reached.

-
- Authentication requirements for all end users and devices to not only restrict access to calling capabilities, but also forcing the end user or device to be managed within the call limitation enforcements stated above.
 - In response to our December 6th, 2024 Failure to Comply notification, we submit the following addition. As a micro-provider, we do not use any third-party analytics vendor and therefore have no vendor to name.

J&J has completed STIR/SHAKEN implementation using its own capabilities, and that of its upstream partners, to ensure not only the ability to mitigate robocalls efficiently, but to also quickly and efficiently track and be notified of any instance of excessive calls either in or out of our VoIP network for the added benefit of Traceback and information co-operation with any and all enforcement agencies named below in the Commitment to Traceback Cooperations section.

Proactive Network Monitoring

J&J has various monitoring and reporting systems in place to analyze traffic on its network for potentially suspicious traffic patterns that are likely to be associated with illegal robocalls or other potentially unlawful usage. For example, J&J's monitoring systems are capable of assessing traffic based on various criteria, including data relating to short-duration calls, answer-seizure ratios, invalid Caller ID ANIs, and anomalous volumes of 404, 503 and other call-failure codes.

If J&J detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, J&J takes prompt action to identify the party that is using its network to carry these calls and take appropriate action. Once suspected unlawful traffic is discovered, J&J blocks any further traffic from the customer and issues an Acceptable Use Violation notice.

Commitment to Traceback Cooperations

J&J commits to timely cooperation with, and responding to, Traceback requests from the ITG (or any successor entity designated by the FCC), trace-forward investigations, and other valid law enforcement and government demands, subpoenas, and other valid legal processes.

J&J will dedicate sufficient resources to provide prompt and complete responses to such requests. J&J will investigate suspicious activity found by its monitoring systems or reported to it by consumers or third parties and take appropriate action.