

200 NETWORKS, LLC ROBOCALL MITIGATION PLAN

I. 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 200 Networks Telecom, LLC. (“200 Networks”), 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 June 30, 2021, in the Commission’s [Robocall Mitigation Database](#) whether they have implemented STIR/SHAKEN or, if subject to an applicable extension, that they have documented and instituted a robocall-mitigation plan to help combat the origination of illegal robocalls on their networks.¹ 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.

200 Networks 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 200 Networks’ Robocall Mitigation plan.

II. 200 Networks’ Know Your Customer (“KYC”) Standards

200 Networks is a voice service provider that focuses its business and operations on the wholesale and business customer segments of the voice services communications market. As part of its customer-onboarding process, 200 Networks undertakes various commercially reasonable precautions to verify a given prospective customer’s identity and relevant business practices as part of entering into a formal written agreement with that customer. All prospective customers must complete a questionnaire which provides 200 Networks with detailed background corporate 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;

¹ See <https://docs.fcc.gov/public/attachments/DA-21-454A1.pdf>.

5. Customer's billing address and all addresses at which customer conducts business
6. Whether the customer engages in telemarketing and, if so, whether the customer delivers prerecorded messages. If the customer engages in telemarketing and delivers prerecorded messages, 200 Networks inquires into whether the prospective customer has evidence of the recipient's prior express written consent to receive these calls;
7. If the prospective customer's business involves the resale or offering of interconnected telephony services or the resale or licensing of telephone numbers, we inquire into the customer's USF registration number.
8. The names of two trade or bank references.
9. If the customer is a telemarketer, a description of the goods and services sold, a list of all caller ID numbers and call back numbers used.

After 200 Networks conducts its preliminary vetting, the prospective customer and 200 Networks schedule and perform test calls over their networks. As part of that process, 200 Networks' personnel personally make test calls to those phone numbers being used as the prospective customer's Caller IDs to, among other things, confirm that the Caller ID rings back to a line associated with the prospective customer and offers callers the opportunity to add the calling party's number to the prospective customer's internal DNC list.

III. 200 Networks' Acceptable Use Policy

As part of its customer-onboarding process, 200 Networks' customers contractually agree to various terms and conditions, including a commitment to comply with 200 Networks' 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 200 Networks' 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.

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

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

200 Networks is diligently pursuing the deployment of STIR/SKAKEN in the IP portions of its network but has not completed that process as of the filing of this Plan. Given 200 Networks' status as a small provider, it is subject to the Commission's two-year extension. 200 Networks' network is capable of accepting and accurately transmitting all STIR/SKAKEN-related data it receives in the call path.

V. Proactive Network Monitoring

200 Networks 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, 200 Networks' 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 200 Networks detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, 200 Networks 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, 200 Networks blocks any further traffic from being carried associated with the Media IP address of that suspicious traffic.

VI. Commitment to Traceback Cooperation

200 Networks 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. 200 Networks will dedicate sufficient resources to provide prompt and complete responses to such requests. 200 Networks will investigate suspicious activity found by its monitoring systems or reported to it by consumers or third parties and take appropriate action.