

RED ROCK COMMUNICATIONS, 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 Red Rock Communications, LLC (“Red Rock”), 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 Red Rock is entitled to the FCC’s extension for small voice service providers. 47 C.F.R. § 64.6304. 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.

Red Rock 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 Red Rock’s Robocall Mitigation plan.

II. Red Rock Communications’ Know Your Customer (“KYC”) Standards

Red Rock is a voice service provider that focuses its business and operations on the termination of voice traffic to business customers that receive voice calls. As such, Red Rock originates very little, if any, traffic. Red Rock nevertheless submits this plan to articulate its policies that would apply in the event it serves customers that originate voice calls.

As part of its customer-onboarding process, Red Rock undertakes various commercially reasonable precautions to verify a given customer’s identity as part of entering into a formal written agreement. All prospective customers participate in an in-person or telephonic enrollment process. Red Rock investigates the prospective customer’s background, such as checking for a company website, the amount of time the business has been open, and confirming their corporate status with the applicable State Secretary of State’s office or website, along with other indications of a legal, operating business. Among other data points collected and, as appropriate, verified, as part of those processes Red Rock Communications gathers the following

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

customer-identifying facts and circumstances:

- Customer business name,
- state or country of incorporation,
- physical business location,
- contact person(s),
- federal tax ID number, and
- FCC Filer ID.

Red Rock's verification practices include confirming a carrier customer's reported status in the FCC's Form 499 Filer database of registered carriers, and, as of June 30, 2021, the Commission's Robocall Mitigation Database. Red Rock also conducts, as applicable, credit checks and reviews references with a prospective customer's other carrier-suppliers. If Red Rock contracts with a customer who originated traffic on its network, it would continue to conduct its preliminary vetting, and the prospective customer.

III. Red Rock Communications' Acceptable Use Policy

As part of its customer-onboarding process, all new Red Rock customers will be required to contractually agree to various terms and conditions, including a commitment to comply with Red Rock's Acceptable Use Policy (AUP). Among other things, this AUP prohibits using the Services to engage in any activities that are illegal, abusive, false, fraudulent, deceptive or misleading. It likewise prohibits using the services in any way that violates applicable laws, which in the robocall context includes 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, or 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. Red Rock's contracts with its customers would stipulate that Red Rock is authorized to suspend and/or terminate all Services in the event of an AUP violation.

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

Red Rock is diligently pursuing the deployment of STIR/SHAKEN in the IP portions of its network but has not completed that process as of the filing of this Plan. Given Red Rock's status as a small provider, it is subject to the Commission's two-year extension. With very limited exception, Red Rock's end users can only use telephone numbers to which they have subscribed from Red Rock, such that Red Rock has a documented, verified relationship between the end user and their telephone number(s) used to receive their calls. In the rare exception in which the Red Rock end user is using numbers secured from a different service provider, Red Rock documents and verifies the end user's right to use the associated phone number(s) from the unaffiliated provider(s).

V. Proactive Network Monitoring

If Red Rock detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, Red Rock would take prompt action to identify the party that is using its network to carry these calls and take appropriate action. If Red Rock detects suspected unlawful traffic is discovered, Red Rock would block any further traffic from being carried associated with the Media IP address of that suspicious traffic.

VI. Commitment to Traceback Cooperation

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