

Granite Telecommunications, LLC

Caller ID Authentication Plan

Introduction. Granite Telecommunications, LLC (“Granite”), pursuant to Sections 64.6301 and 64.6305 of the Commission’s rules, 47 C.F.R. §§ [64.6301](#), [64.6305](#), and the Commission’s “Best Practices” adopts this Caller ID Authentication (“Plan”). This Plan is current as of its revision date and may be subject to change to comply with Commission regulations and requirements, as may be amended.

Commitment. Pursuant to Section 64.6305 of the Commission’s rules, 47 C.F.R. § [64.6305](#), Granite commits to take all such reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond fully and in a timely manner 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. As set forth below, Granite has adapted the North America Numbering Council Call Authentication Trust Anchor Working Group’s *Best Practices for the Implementation of Call Authentication Frameworks* (“Best Practices”) into its Plan.

Compliance. Granite is deemed a provider of “voice service” as set forth in Section 64.6300(l) of the Commission’s rules, 47 C.F.R. §64.6300(l). Granite certifies that all voice traffic that originates on its network is authenticated under the STIR/SHAKEN authentication framework, pursuant to 47 CFR § 64.6301(a). Granite has implemented DNO blocking compliant with (47 CFR § 64.1200(o). For all voice traffic, including traffic that originates on underlying carrier networks over which Granite lacks control of the network infrastructure necessary to implement the STIR/SHAKEN authentication framework, Granite internally performs Subscriber Vetting, Telephone Number Validation, and Network Traffic Monitoring, Analysis and Investigation as set forth below, in conjunction with its underlying carrier caller ID authentication frameworks. In addition, Granite certifies that, in addition to functioning as a voice service provider, Granite may operate as an intermediate provider within the meaning of 47 C.F.R. §64.6300, and remains in full compliance with all applicable obligations as set forth in 47 C.F.R. §64.6301 and §64.6305.

Caller ID Authentication Plan. In accordance with the Best Practices, the following constitutes Granite's Caller ID Authentication Plan:

Company Information

The name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues is as follows:

Geoff Cookman
Director of Carrier Relations
Granite Telecommunications, LLC
1 Heritage Drive
Quincy, MA 02171
Telephone: 617-933-5521
Email: regulatory@granitenet.com

Granite does not operate under an assumed name. Granite serves customers located in the United States, its territories, and Canada.

Authentication

Granite has call authentication that complies with caller ID authentication requirements for voice traffic originated on its network. Granite digitally signs outbound calls to battle spoofing and assure customers of legitimate calls. Granite also utilizes analytics to detect illegal calls, and applies call treatment by overwriting the caller ID with "SPAM ?" or "Fraudulent Call" based on the fraud score; generates fraud alerts, block suspected illegal calls, and enables reporting via a data analytics dashboard.

Granite identifies Toll Free and Local Numbers that should not be receiving calls, and that provide automated and ad hoc reporting to analyze traffic patterns and calling data such as average call duration, Answer Seize Ratio ("ASR"), total calls to unique numbers etc.

Granite also proactively distinguishes communications fraud from legitimate customer usage to help combat fraud schemes. This is done by employing dynamic usage profiling and other monitoring metrics to identify suspicious activity regardless of the manner in which unauthorized access was gained.

Granite further performs the following functions internally to authenticate its subscriber callers:

Know Your Customer

Granite vets subscribers before providing service and any customers that are a "voice service providers" or "intermediate provider" must be in the Robocall Mitigation Database. Granite obtains specific subscriber information which may include but not be limited to service locations, Tax ID for a credit check, and contact person(s) and principals. Further, Granite compares information provided by the subscriber against underlying carrier records to verify accuracy and authentication and validate subscriber information. Subscribers are served under a service agreement, online Terms of Service, and/or a Moderation of Use and Acceptable Use Policy.

Telephone Number Validation

For new subscribers, Granite may assign telephone numbers to the subscriber and/or the subscriber may port telephone numbers from another service provider. Granite ensures that only those subscriber telephone numbers held by its subscribers may originate traffic (with some exceptions for specifically negotiated services for certain customers). For toll-free numbers, Granite verifies the underlying ten-digit number and ensures that only calls from the assigned numbers may originate calls. Granite can trace calls directly back to the customer's network/IP.

Network Traffic Monitoring, Analysis and Investigation

Granite monitors its subscribers' traffic for call, originating number and terminating number irregularities in conjunction with its underlying carriers, and should irregularities be determined, will promptly contact the subscriber as part of its investigatory process.

Granite is coordinating with its underlying carriers to monitor subscribers' traffic, identify traffic anomalies for which Granite will investigate, and to promptly block subscriber service if robocalling is suspected. Detection of illegal activity and violations will result in service termination.

Granite monitors its networks in real-time, allowing it to identify suspicious network activity (based on abnormal call patterns, atypical call activity, hot lists, and subscriber information). Granite stops unwanted events by blocking at its switches and can tear down active calls. There are automatic alerts and automatic disabling set up based on predefined parameters. Granite's systems allow it to create ad hoc reports as well as automated custom reporting and alarms with detailed call analytics to examine suspicious traffic patterns and usage statistics.

Response to Traceback Requests

Consistent with its commitment above, Granite will respond fully and in a timely manner 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.

Customer Contracts

Provisions in customer contracts, tariffs, and service guides prohibit any unlawful, abusive or illegal use of services. Contractual provisions also provide Granite the right to suspend or interrupt service that is being used to violate these policies. Granite will seek to identify the party that is using its network to originate such calls and take appropriate action under the customer's contract. Granite has updated its terms of service to expressly include a prohibition on the use of the service in any illegal, fraudulent, improper, inappropriate, and/or unauthorized manner.

Customer and Employee Awareness

Granite has a STIR/SHAKEN and Robocalling Mitigation Team focused on compliance and awareness. Granite has documentation available to customers and employees explaining STIR/SHAKEN, robocalling mitigation and fraud. This documentation explains the products, procedures and methods we use to combat fraud and robocalling. Information about STIR/SHAKEN and Robocalling Mitigation has been distributed and is available companywide.

Ongoing Robocall Mitigation

Granite anticipates that its Plan will evolve as it makes Plan enhancements, as underlying carriers enhance their own plans, and as the Trust Anchor and industry generally gain experience in caller ID authentication protocols.

Granite intends to promptly amend its compliance plan as changes may occur.

February 19, 2026

Granite Telecommunications, LLC

/s/ Geoff Cookman

Geoff Cookman
Director Carrier Relations
Granite Telecommunications, LLC
1 Heritage Drive
Quincy, MA 02171