

Cannon VoIP Robocall Mitigation Program Description

1. Overview

Cannon VoIP ("Company") is a domestic voice service provider that originates voice traffic to the public switched telephone network in the United States. Company has implemented a comprehensive robocall mitigation program designed to take reasonable and effective steps to prevent the origination of illegal robocall traffic on its network and to comply with all applicable Federal Communications Commission (FCC) rules and orders regarding robocall mitigation and caller ID authentication.

2. STIR/SHAKEN Implementation

Company has implemented the STIR/SHAKEN caller ID authentication framework on the Internet Protocol (IP) portions of its network where technically feasible and appropriate. For calls that traverse IP segments where STIR/SHAKEN can be applied, Company authenticates caller ID information and attaches appropriate attestation levels in accordance with industry standards.

For any calls that cannot yet be authenticated with STIR/SHAKEN (e.g., due to legacy TDM interconnections or technical limitations), Company subjects such traffic to the robocall mitigation measures described in this plan.

3. Know-Your-Customer (KYC) Procedures

Company maintains and enforces written Know-Your-Customer procedures to reduce the risk that its services are used to originate illegal robocalls. These procedures include:

- Collecting and verifying customer identity information (e.g., legal name, physical address, corporate registration, tax identification, and contact details) prior to activation of voice services.
- Evaluating customer use cases and expected traffic patterns, including target geographies, call volumes, and calling profiles.
- Screening prospective high-risk customers (such as outbound-only dialers, lead generators, and call center operators) with enhanced due diligence, which may include reference checks, web presence review, and confirmation of any required state or federal registrations.
- Requiring acceptance of contractual terms that expressly prohibit illegal robocalls and abusive calling practices, and that permit Company to suspend or terminate service upon evidence of such activity.

4. Caller ID and Numbering Controls

Company enforces controls over caller ID usage to prevent spoofing and other misuse:

- Assigning telephone numbers to customers from authorized number resources under Company's control or from trusted upstream providers.
- Restricting customers to use only caller ID numbers that they have been assigned by Company or for which they have demonstrated valid authorization.

Cannon VoIP Robocall Mitigation Program Description

- Implementing technical measures to validate caller ID values presented in SIP signaling and to prevent use of unauthorized or invalid numbers where feasible.
- Maintaining and applying reasonable do-not-originate (DNO) lists (for example, invalid, unassigned, or known non-dialable numbers) to block clearly invalid calls before they reach the PSTN.

5. Traffic Monitoring and Analytics

Company actively monitors outbound call traffic to detect patterns indicative of illegal robocalling, including:

- Monitoring call volumes, call attempts per second, average call duration, and answer rates at the customer, trunk, and route level.
- Flagging and reviewing traffic that exhibits anomalous or high-risk characteristics, such as extremely short call durations, very high call-per-second rates, or concentrated calling to particular number ranges.
- Using internal tools and, where applicable, third-party analytics to identify suspicious traffic patterns and potential illegal robocall campaigns.
- Periodically auditing traffic of higher-risk customers and use cases for compliance with this plan and applicable law.

6. Response to Suspected Illegal Traffic

When Company identifies, or is notified of, potentially illegal robocall traffic originating on its network, it takes prompt remedial action, which may include:

- Immediately investigating the traffic, including review of call detail records, call samples where available, and relevant customer information.
- Contacting the customer to obtain an explanation and, where appropriate, requiring corrective measures or changes in calling practices.
- Implementing interim controls such as rate-limiting, restricting destinations, or tightening caller ID constraints while the investigation is underway.
- Suspending or terminating service to customers that engage in, facilitate, or fail to remediate suspected illegal robocalling activity.
- Updating internal risk ratings and controls for customers found to be associated with problematic traffic.

7. Cooperation with Traceback Requests and Authorities

Company fully cooperates with the Industry Traceback Group (ITG), the FCC, law enforcement, and other authorized entities in investigating suspected illegal robocalls. Company:

- Responds to traceback requests in a timely manner and provides all available, relevant information consistent with applicable laws and privacy obligations.
- Traces back calls through its network to the originating customer or upstream provider to the extent technically and legally feasible.

Cannon VoIP Robocall Mitigation Program Description

- Takes appropriate remedial action, as described above, when traceback results indicate that a customer or upstream provider is associated with illegal robocall traffic.

8. Upstream and Downstream Provider Management

Company takes reasonable steps to ensure that its upstream and downstream carrier relationships support robocall mitigation objectives:

- Where Company obtains services from upstream providers, Company prefers partners that are listed in the Robocall Mitigation Database and that have adopted robust robocall mitigation practices.
- Company evaluates and, where appropriate, limits traffic from upstream partners that demonstrate patterns associated with illegal robocalling.
- Company provides relevant robocall-related information to downstream interconnecting carriers as needed to support industry-wide mitigation efforts.

9. Ongoing Review and Program Enhancement

Company's robocall mitigation program is an ongoing effort. Company:

- Periodically reviews its mitigation measures, policies, and tools to account for changes in regulatory requirements, enforcement guidance, and industry best practices.
- Trains relevant personnel on robocall mitigation responsibilities, procedures, and escalation paths.
- Updates this plan and related internal procedures as necessary to improve effectiveness and maintain compliance with FCC rules and orders.

10. Certification

A corporate officer of Company, with responsibility for oversight of robocall mitigation compliance, has reviewed this plan and certifies that Company has implemented the above-described robocall mitigation program for all calls it originates that are not fully authenticated with STIR/SHAKEN, and that the information included in Company's Robocall Mitigation Database filing is true, accurate, and complete to the best of that officer's knowledge and belief.

4-3-2026

Brayden Cannon

Owner/Founder

Cannon VoIP