



Robocall Mitigation Plan

Final document date: April 19, 2024

Background

In 2020, the Federal Communications Commission (FCC) issued rules requiring that certain communications service providers implement the STIR/SHAKEN call authentication framework and other robocall mitigation practices, generally by June 2021. A key element of the FCC rules is a requirement for all voice service providers to certify as to the status of their implementation of STIR/SHAKEN and, if the provider has not fully implemented the framework (including providers excused due to an extension), the provider must implement a robocall mitigation program on the exempted portions of its network.

There are three required elements of a robocall mitigation program:

1. the provider must take reasonable steps to avoid originating illegal robocall traffic
2. the provider must commit to respond to requests from the Industry Traceback Group to trace suspect calls for mitigation efforts; and
3. the provider must cooperate in investigating and stopping any illegal robocallers.

These plans should be customized and should reflect the service provider's customer base, services and the risk that illegal robocalls may be originated on its network. This document describes Bitnetix's Robocall Mitigation Plan (RMP).

About Bitnetix

Bitnetix Incorporated (dba, "SmartVox") is a small provider of Voice over IP (VoIP) services to non-profits and small businesses. Our customers are typically professional service companies such as attorneys, accountants, and service organizations. Our footprint is primarily in Western New York, but we have customers across the United States.



Customer Due Diligence

Bitnetix's customers are not of a type that typically engages in large call volume or robocall-related call tendencies. Primarily, our customers use our service for inbound calling rather than outbound calling, and are a mixture of legal and financial services, religious organizations, counselling and victim resource organizations, and a handful of small "mom and pop" businesses.

Bitnetix staff personally knows each and every customer. None of our customers have the call path capacity to generate the high volume of traffic associated with robocalling. In addition, our in-house real-time monitoring analyzes and alerts to suspicious behavior, shutting it down automatically and notifying staff of potential violations.

We do not deploy capacity for residential customers. We require a tax ID and verification of the business for each customer. For non-profit customers, we require proof of non-profit status.

Terms of Service

New customers are required to agree to our Terms of Service (ToS) which specifically states, without being limited to, that our service:

- Will not be used for any excessive business use including, but not limited to, auto-dialing, continuous or extensive call forwarding, continuous connectivity, fax broadcasting, fax blasting, telemarketing (including without limitation charitable or political solicitation or polling), automatic dialing, call centers, public calling centers or internet cafes or any other activity that would be inconsistent with normal small business usage patterns.
- Shall be used only for lawful purposes.
- Shall not be used in any way that is threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, invasive of another's privacy, or any similar behavior.

We reserve the right to immediately disconnect a customer's service without notice, if, in our sole and absolute discretion, we determine that they have used the Service or any Device in violation of our ToS.

Network Monitoring

Bitnetix is an IT consulting company, of which our SmartVox VoIP platform is but a part. Bitnetix also provides monitoring and notification services. Our real-time monitoring software examines traffic, call patterns, and SIP connections and automatically detects attacks, suspicious behavior, or call patterns that do not match a customer's previous usage.



Automated Call Management

Bitnetix has a central list of blocked calls that we will not accept into or out of our system for any customer. This includes calls that originate from an invalid number, a globally identified "black list," or calls which appear to route through our platform without being initiated by our platform.

Upstream Provider

We primarily use one upstream provider for all of our termination to the PSTN. This provider has their own STIR/SHAKEN policies and robocall mitigation. Calls from our service are signed with our unique ID and our provider will provide attestation for outbound call services. Calls without valid originating numbers - either missing or an incorrectly formatted number (not 10-digits) - will be rejected by our system and not passed on to our provider.

For inbound calls, we provide the verstat ID in signaling, and the option to provide signed call delivery indication via CNAM presentation. Additional call treatment features are under development and will be made available later as a value-added service from our provider.

Traceback and Enforcement Cooperation

Bitnetix will actively cooperate with the traceback community including the FCC, law enforcement, and The Industry Traceback Group (ITG) to investigate and stop illegal robocalls. We will dedicate sufficient resources to provide prompt and complete responses to traceback requests. Failure for a customer to comply with our ToS or to be identified as origination illegal calls will have service terminated as per our ToS.