



Robocall Mitigation Plan (RMP)

Title	Date
Robocall Mitigation Plan	2/19/2026

Version 1.3

Prepared by: David A. King

Number Sentry, LLC
107 Technology Parkway
Suite 220
Peachtree Corners, GA 30092

Revision Log

Version	Date	Change	Author
V1.0	9/22/2021	Initial version	D King
V1.1	5/3/2022	Updates in preparation for providing outbound voice services	D King
V1.2	2/26/2024	General Updates	D King
V1.3	2/19/2026	General Updates	D King

1. Overview

The Federal Communications Commission (FCC), as part of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, requires that all Voice Service Providers register in the Robocall Mitigation Database (RMD). This registration certifies that the VSP has fully implemented STIR/SHAKEN or, alternatively has implemented a Robocall Mitigation Plan to ensure they are not originating illegal robocalls from their customers.

Number Sentry is dedicated to stopping illegal robocalls from originating from our network and to monitoring incoming traffic terminating on our network to help identify illegal traffic from ‘bad actors’.

2. Purpose

In addition to a variety of related services, Number Sentry provides both originating and terminating voice traffic on behalf of some of its customers. Accordingly, this Robocall Mitigation Plan is being updated and filed in the RMD.

The following is a list of “Mitigation strategies” have been implemented by Number Sentry.

3. Customer Contracts

All customers for whom Number Sentry provides Voice Origination services, Voice Termination Services or Telephone Numbers (DIDs) must sign the company’s Terms and Conditions prior to using these services. Amongst other things, the Terms and Conditions prohibit:

- a. Using any Number Sentry service to engage in deceptive, fraudulent, or otherwise illegal practices
- b. Use of any Number Sentry service to aid or render violations of any applicable local, state, or federal law
- c. Providing false or misleading information about the identity of the customer or the origin of any outbound call
- d. Other uses of any Number Sentry service that are outside of accepted industry practices and guidelines for call origination or termination

4. Know Your Customer (KYC)

Knowing your customer is foundational to stopping illegal robocalls from originating from our network and to identifying and stopping illegal traffic from ‘bad actors’. Thus, Number Sentry dramatically strengthened its Know Your Customer (KYC) process in 2025. Number Sentry’s KYC process is based on both qualitative measures as well as quantitative metrics to provide the highest degree of certainty that our outbound calling products and services are properly employed. Every Number Sentry prospective client must complete an exhaustive KYC process. This KYC process even includes prospects who do not intend to use Number Sentry’s voice services. The KYC Application process initiates a multi-step vetting process as follows:

- A. The KYC process is initiated when a prospective client completes an online KYC form. This form asks which Number Sentry services the prospect is interested in and collects substantial information related to the business, its web-based properties (website, social media, etc.), USA physical location, line of business, executive contacts, and more. Prior to submitting KYC information, the submitter is required to attest to the truth and accuracy of the KYC information they provide.
 - i. Existing clients are also provided with the capability to update their KYC details should they wish to request additional Number Sentry services, or to report any change in their previously submitted KYC details.
- B. KYC Applicant Submissions are distributed to the Number Sentry KYC team, which always includes a minimum of two (2) members of the Executive team.
 - i. Additionally, all submitted KYC information is tracked in an internally accessible KYC Management portal. This KYC Management portal is accessible to the Number Sentry KYC team, The Number Sentry Sales team, the Number Sentry Care team, as well as other key personnel.
- C. Upon receipt of a KYC Applicant Submission (or update of an existing client’s KYC details), Number Sentry KYC staff verify the KYC submitted information using a KYC Confirmation Template. This template assigns a point value and a weight to each piece of information gathered on the KYC form, and to information gathered about the KYC applicant from other third-party sources.

- D. KYC staff proceeds to verify the KYC Applicant's Submission using the KYC Confirmation checklist and third-party sources. As each piece of KYC information is verified, the KYC Applicant is assigned a score for that component of the KYC Confirmation template. The score represents the level to which KYC personnel were able to verify the data provided by the KYC Applicant for each item in the KYC Confirmation template. These scores are then multiplied by the weight of assigned to each component to calculate a point score for each component of the KYC Confirmation template. The weighted scores for each component of the KYC Confirmation template are added together to determine the KYC Applicant's overall KYC score. The result of the completed KYC Confirmation Template is a weighted attribute KYC 'scorecard' that provides a quantitative assessment of the KYC Applicant.
- E. KYC Approval is broken into 3 levels. The lowest level is "test-only". The next level is "non-origination", and the most stringent level is "full approval". The point value of the KYC Applicant's KYC scorecard determines the level of KYC Approval the KYC Applicant is eligible to receive.
 - i. Furthermore, every service provided by Number Sentry, including both voice origination and termination services as well as non-telecommunication services, is assigned a minimum KYC approval level. Some services require only "test-only" approval, others require the higher KYC Approval level of "non-origination" and other services, including those that enable outbound calling, require the highest level of KYC Approval, "full approval".
- F. Based on the services requested by the KYC Applicant and their KYC scorecard results, Number Sentry KYC staff approve, reject, or partially approve the KYC Applicant's KYC Submission using the KYC Management portal. Note that a partial approval indicates the KYC Applicant did not score high enough to receive approval for all services that they requested.
 - i. When the KYC Management portal is updated with the KYC Applicant's approval level, the KYC team and the KYC Applicant are notified of the approval, rejection (and reason for the rejection) or the partial approval of the KYC Applicant.
 - ii. For approvals or partial approvals, the KYC Applicant's Number Sentry account is then built, and the appropriate, approved services are assigned to the client.

This comprehensive, quantitative KYC process allows Number Sentry to scrutinize their customers' business details. Number Sentry also attempts to ensure that the calling patterns of users of Number

Sentry voice services are well within the caller identity guidelines as described by the NANC Call Authentication Trust Anchor Working Group and are not using illegal calling practices.

5. STIR/SHAKEN Implementation

Number Sentry has fully implemented the Stir/Shaken call authentication and verification process for all outgoing calls. Number Sentry signs and properly “attests” every call that originates on our network.

6. Ongoing Monitoring

Voice traffic related metrics for Number Sentry call origination services are routinely performed to identify patterns consistent with illegal robocalls. Traffic metrics such as Average Length of Call (ALOC), Answer Seizure Rates (ASR) and other Call Detail Record (CDR) based call pattern analysis are automatically updated. Such metrics, along with feedback from third-party Analytic Provider testing aid Number Sentry by ensuring our Voice Origination services and Voice Termination services are utilized in a manner consistent with legal calling practices.

Should a customer exhibit indications of illegal calling practices, Number Sentry will take appropriate actions to stop such calls. Such actions may include but are not limited to:

- a. Notifying the customer of the degradation of their Traffic Metrics and working together to identify the source of the degradation
- b. Blocking outbound traffic from suspicious telephone numbers
- c. Suspension of Number Sentry call origination services for that customer
- d. Termination of Number Sentry call origination services for that customer
- e. Other measures as deemed appropriate by Number Sentry to prevent illegal robocalls from originating from our network

7. Traceback Requests and Response to Suspicious Activity

Number Sentry will respond to all traceback requests fully, and in a timely manner, from the Commission, law enforcement, and the registered traceback consortium. In addition, Number Sentry will

cooperate with such entities to facilitate vigorously investigating and stopping any abusive Robocallers and Scammers that attempt to use the Number Sentry network to originate or terminate calls