

Robocall Mitigation Plan

Business Information

Numberify, Inc
1608 Nogales St #C08
Rowland Heights CA 91748

Contact Information

Michael Lee
CEO
(626) 365-0888
michael@numberify.com

Overview

In the Commission's release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (rel. March 17, 2023) ("R&O") it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outline "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that a RMP include:

- "know your customer" procedures;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

Purpose

Numberify, Inc ("Numberify") is a small VSP dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network.

As certified in the FCC's Robocall Mitigation Database, Numberify has fully implemented STIR/SHAKEN. In compliance with the R&O, Numberify submits this RMP and certification.

Know Your Customer ("KYC")

To subscribe to Numberify's services, potential subscribers are required to complete a comprehensive KYC form. This form captures essential information including, but not limited to:

1. Full legal name of the individual or business entity.
2. Contact information, including address, email, and phone number.
3. Valid identification for individuals or registration documents for businesses.
4. Intended use of Numberify's services must be consistent with personal communications for consumer end users. Consumer messaging functionality, where enabled, is limited exclusively to manually initiated Consumer (P2P) communications between individuals. Separate business voice services may be provided on a limited basis for voice-only communications and do not include SMS/MMS functionality.
5. Payment information and intended usage levels.

Consumer Communications Platform:

Numberify primarily provides consumer-facing communications services for individual end users through its consumer application platform. Consumer onboarding is completed online using identity verification, payment verification, CAPTCHA, and account security controls.

Messaging functionality, where enabled, is limited exclusively to manually initiated Consumer (P2P) communications between individuals. Numberify does not support A2P, bulk, automated, marketing, notification, or business messaging.

Business voice services, where provided, are separate from the consumer messaging platform and are limited to voice-only communications. SMS/MMS functionality is not enabled for business voice accounts.

Messaging Scope (Consumer P2P)

Messaging may include incidental service-related communications initiated by the end user. Systematic, high-volume verification traffic, automated account creation, or verification-focused use is prohibited and subject to enforcement action.

Numberify provides Consumer (P2P) messaging, where enabled, exclusively to individual end users through its consumer application. Messaging is limited to one-to-one, manually initiated communication between individuals. Consumer messaging services are intended for interpersonal communications between individual end users and are not designed or marketed for enterprise or application-driven communications.

Numberify does not support A2P, bulk, automated, marketing, or business messaging. Business voice accounts do not have SMS/MMS enabled.

In limited cases involving separately vetted voice-only business accounts, enhanced verification procedures may apply where appropriate. These procedures do not apply to consumer application users. Business voice accounts remain separate from the consumer messaging platform and do not have SMS/MMS functionality enabled.

Regarding payment restrictions, we assess each subscriber's needs and usage forecasts to determine appropriate limits on the amount and frequency of payments. This is done to prevent any unusual or potentially fraudulent activity. In addition to manual assessment, Numberify enforces automated payment, usage, and message volume thresholds to identify and prevent anomalous or abusive behavior.

We follow the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group.

This process includes the collection and review of entity-identifying information to confirm that we have an authenticated relationship with the customer. We use this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

We also validate, when possible, that the entity has a legitimate right to use its asserted calling numbers. We use this information to support the attestation level we assign to calls that we originate for that customer.

Our commitment to knowing our customers extends beyond these initial steps. We maintain ongoing monitoring and communication with our subscribers to ensure continued compliance and to address any changes in their service requirements.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking In CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59* (Rel. May 19, 2023) ¶¶ 49-51, Numberify provides the following information concerning its upstream voice service carrier.

Numberify has two upstream providers from which it receives voice traffic:

Inteliquent, Inc. DBA Onvoy, Sinch
550 W. Adams St.
Suite 900
Chicago, IL 60661
Stacy Graham
Stacy.graham@sinch.com

Bandwidth Inc.
900 Main Campus Drive
Suite 100
Raleigh, NC 27606
Stephen Thayer
voicesecurity@bandwidth.com

Numberify is working with its upstream provider diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

Numberify maintains an AUP that subscribers must agree to before being permitted to use Numberify's software and services. Among other things, the AUP prohibits:

- using our service for any illegal purposes whatsoever;
- engaging in activity for which FCC or any equivalent national regulatory authority has restricted or regulated in relation to proper use of the public telephony network or the Internet;
- using our service if Numberify determines, at its sole discretion, that its provision for this customer is prohibited by applicable law or has become impractical or unfeasible for any legal or regulatory reason; and
- using our service to offer or otherwise make available to others fraudulent goods, services, schemes, or promotions, including make-money-fast schemes, Ponzi and pyramid schemes,

phishing, pharming, harvesting or similar deceptive practices.

Our contractual provisions with customers prohibit them from initiating illegal robocalls. If we identify suspicious or illegal robocall activity, Numberify may automatically restrict or suspend service in real time pending investigation. If the activity is confirmed or continues, we terminate service.

Telephone Number Authorization

New subscribers placing outbound calls can only use Caller IDs which have been assigned and provisioned through our platform or ones verified through automated-number-validation voice call. Subscribers can sign a form allowing them to use Caller IDs not assigned through our platform or verified by validation call for outbound calls, functionality that is restricted to separately vetted voice-only business accounts subject to enhanced verification procedures. This process does not apply to consumer application users and is restricted to vetted business voice customers only.

Analytics for Monitoring Traffic

Numberify works to detect a calling pattern consistent with illegal robocalls. If such a call is detected, we will identify the party that is using our network to originate those calls and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our network.

We use call analytics software provided by TransNexus to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls.

The software provides detailed reporting to identify suspected illegal robocalls. The system alerts us if we process outbound calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list. Calls originating from numbers listed on industry-recognized or regulator-provided Do Not Originate (DNO) lists are blocked from origination on Numberify's network.

We perform the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call.

We immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. We employ automated rate limits, behavior-based triggers, and anomaly detection to help identify and contain suspicious activity pending investigation. If we determine traffic is likely unlawful, Numberify may automatically restrict or suspend service pending investigation. If the activity is confirmed or continues, we terminate service.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Numberify's risk prevention team is alerted, which follows the defined procedures on investigating such subscribers.

The procedures established include, but are not limited to:

- Monitoring and Detection;
- Immediate Investigation;

- Subscriber Verification and Contact;
- Temporary Suspension of Services

Blocking

Numberify will promptly respond to Do Not Originate requests it receives from the ITG. If Numberify's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Numberify will take appropriate action which may include suspending or terminating the subscriber's use of Numberify's network. Numberify will cooperate with investigative bodies (provide a single point of contact to address traceback requests from law enforcement including state attorneys general offices), to the FCC, and/or the ITG; as well as documenting requests and actions taken in response thereto.

We respond within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. We cooperate fully with such entities in investigating and stopping any illegal robocallers that use our service to originate, carry, or process illegal robocalls.

Plan Updates

This plan and industry best practices must evolve in response to the dynamic nature of mitigating illegal robocalling. Numberify will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

In the event of any material change to this plan, Numberify will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of Michael Lee

I, Michael Lee, the CEO of Numberify, do hereby certify, under penalty of perjury, the following:

- (1) Numberify has fully implemented STIR/SHAKEN in the IP portions of its network.
- (1) Numberify's Business name and primary address are as follows:

Numberify, Inc.
1608 Nogales St #C08
Rowland Heights CA 91748
- (2) Numberify has no other business names in use.
- (3) Numberify is 100% owned by me, Michael Lee. I have not had any licenses/authorizations revoked, nor have I been subject to any other FCC enforcement actions.
- (4) Numberify previously used the business names Minghai, Inc. and Number Republic, Inc.
- (5) The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- (6) Numberify's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (7) Numberify has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (8) Numberify is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (9) Numberify's Operator Code Number is 837k.



Michael Lee