



Robocall Mitigation Plan

Purpose and Table of Contents

Vonage's Robocall Mitigation Plan sets forth the actions Vonage takes to:

- I. SCREEN its customers prior to providing voice services ("Know-Your-Customer");
- II. MONITOR existing customers for traffic patterns and other information indicative of either having the potential to transmit fraudulent robocalls or actually transmitting same; and
- III. MITIGATE the transport of fraudulent robocall traffic via Vonage.

I. SCREEN

Vonage undertakes the following Know-Your-Customer ("KYC") activities prior to providing voice services:

A. **Information Collection.** All Vonage customers must provide their names, addresses, verified e-mail address(es), verified phone number(s), validated payment information, and, if the customer is a legal entity, the state or country of formation, contact person, and company registration number.

B. **Information Validation.** Vonage verifies the information obtained from the customer through the collection and validation of the following documentation:

1. **Proof of Identity:** A digital copy of a current valid government issued form of identification for the applicant, such as a passport or driver's license.
2. **Proof of Residence:** If an individual, a lease, mortgage statement, recent public utility bill in the customer's name, or other documentation establishing residence.
3. **Proof of Business Legal Entity:** If a business, official documentation verifying the existence of the legal entity and registered address, which may be a copy of one of the following: business license, registry of a non-profit organization, notarized business lease, articles of incorporation, company tax number/ID/EIN or other documentation appropriate to the customer's country of operations. SEC filers may supply their CIK code, which can be verified via the SEC website.
4. **Proof of Authorized Individual:** If a business, official documentation verifying that the individual purporting to act on behalf of the business has the authority to do so. This proof may include a copy of a letter of authority, board minutes or other suitable documentation, or public registration information.

C. **Contractual Provisions.** Customers must agree to Vonage's terms of service that prohibit fraudulent traffic. Additionally, the terms of service provide that Vonage may suspend or terminate services for violating Vonage's acceptable use provisions. Customers may also be held liable for any financial penalties imposed on Vonage for fraudulent traffic sent from the customer.

D. **Know Your Upstream Provider.**

1. **Procurement Processes.** Vonage has a robust procurement process that includes sanctions screening and collecting documentation and information

about its upstream providers that includes, but is not limited to:

- a. W-9s;
 - b. Contact Person(s);
 - c. State or country of incorporation; and,
 - d. Federal tax identification number.
2. **Contractual Terms.** Vonage's contracts with upstream providers require that the provider comply with all relevant laws, including in many instances specific provisions prohibiting the transmission of fraudulent traffic and robocalls. Vonage's contracts also permit Vonage to terminate the upstream provider's right to send traffic to Vonage if any contractual provision is violated.

II. MONITOR.

A. **Traffic Patterns.** Vonage has a dedicated fraud team that continuously monitors its customers' traffic patterns for indicators of fraudulent calls, such as:

1. Short duration calls less than 6 seconds long;
2. Multiple calls per minute from the same customer;
3. Low call answer rates for calls from a particular customer;
4. Calls to high fraud destinations;
5. Dialing patterns;
6. Calls to numbers on Do-Not-Call lists;
7. Traceback requests; and
8. Unusual changes in a customer's established traffic patterns.

B. **SPAM Labeling.** Vonage uses a third party vendor, Neustar, for monitoring its traffic and identifying likely fraud. Certain customers will receive a "spam" indicator prepended to their CNAM display if they receive a call from a suspected robocaller. The spam indicator is based on a proprietary combination of indicators assembled by Neustar.

III. MITIGATE

A. **Commitment to Respond to Traceback Requests.** Vonage commits to respond fully and within twenty-four (24) hours to traceback requests from law enforcement, the Federal Communications Commission, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocalls that use its services to originate such calls.

B. **Robocall Mitigation Database Filings.** Vonage checks the Robocall Mitigation Database and only accepts calls from the following categories of providers if those providers' filings appear in the Robocall Mitigation Database and that filing has not been de-listed pursuant to an enforcement action:

1. Domestic voice service providers;
2. Foreign voice service providers or foreign intermediate providers that use North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States; and,
3. Gateway providers.

C. **Blocking/Discontinuance.** Vonage employs a variety of effective measures to block fraudulent calls. When Vonage identifies actual fraudulent traffic or traffic with a high likelihood

of being fraudulent, its fraud team takes prompt action to block such traffic. In addition to blocking the offending traffic, Vonage may suspend or terminate the offending customer's service.

D. Selective Call Blocking. Certain Vonage products have selective call blocking that rejects or sends to voicemail incoming calls based on their risk profile determined by STIR/SHAKEN validation status and Telephone Number (TN) validation.

This Robocall Mitigation Plan describes the specific measures that Vonage has implemented as of February 26, 2024. Vonage continually evaluates the efficacy of its measures to combat bad actors and takes appropriate steps to improve these measures when needed.