

CarrierX
Robocall Mitigation Plan
(February 2024)

Introduction

This Robocall Mitigation Plan (RMP) details the reasonable steps and actions taken by CarrierX ("CarrierX") to mitigate and eliminate illegal robocalling. CarrierX has an ongoing commitment to identify and help alleviate illegal robocalling by pre-qualifying prospective customers, monitoring existing customers for traffic patterns indicative of prohibited robocalls, and working with other providers and regulatory agencies in combatting fraudulent voice activity.

CarrierX provides originating and terminating voice services. All calls that originate on its network are subject to a robocall mitigation program. CarrierX has fully implemented STIR/SHAKEN and other robocall mitigation efforts.

The Company is not a foreign voice service provider.

The Company does not sell services to international call originators using North American Numbering Plan Numbers.

Compliance History

In the past two years, the Company (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has not been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

No prior RMD certification has been removed by the Commission. The Company has not been prohibited from filing in the Robocall Mitigation Database by the Commission.

The person within the Company responsible for addressing all robocall mitigation-related issues, is:

Name: Bryan Petersen

Title: Chief Network Officer

Department: Operations

Telephone Number: 877-482-5838

Email Address: bryan@carrierx.com

STIR/SHAKEN Implementation

CarrierX has fully implemented the STIR/SHAKEN authentication framework across the entire IP portion of its network, and all calls it originates are compliant with § 64.6301(a)(1) and (2).

The Company does not use a third-party vendor carrier to sign its calls and has its own token.

The Company does not use a third-party call analytics vendor.

Traceback Requests

CarrierX will respond to Traceback requests from the ITG (or any successor entity designated by the FCC), trace-forward investigations, and other valid law enforcement and government demands, subpoenas and other valid legal processes in a timely manner. CarrierX will dedicate sufficient resources to provide prompt and complete responses to such requests. CarrierX will investigate suspicious activity found by its monitoring systems or reported to it by consumers or third parties and take appropriate action. CarrierX is committed to responding fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to co-operating with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. CarrierX has also worked with the FTC and state attorney general counsel to participate in traceback efforts, further demonstrating its commitment to such important efforts.

The Company's point of contact to handle traceback requests is:

Name: David Stoos

Title: Director Network Operations

Email Address: tickets@carrierx.com

Know Your Customer/Know Your Upstream Providers

CarrierX, as part of its customer onboarding process, undertakes various commercially reasonable precautions to verify a given customer's identity, including the following:

- credit references;
- general references;
- meeting with personnel of the customer company; and
- industry standard credit card validation and fraud checks

As part of its customer-onboarding process, as applicable, CarrierX's customers contractually agree to various terms and conditions, including a commitment to comply with CarrierX's Terms

of Service (TOS). All CarrierX customers agree: (i) to comply with all United States laws, rules, and other regulations applicable in connection with the Services; (ii) not to use the Services for illegal purposes; (iii) not to interfere or disrupt networks connected to the Services including by introducing viruses or other technologically harmful materials; (iv) not to use the Services to infringe any third party's copyright, patent, trademark, trade secret, or other intellectual property rights or rights of publicity or privacy; and (v) not to transmit, through the Services, Feedback or otherwise, any unlawful, harassing, libelous, abusive, threatening, harmful, vulgar, obscene, or otherwise objectionable material of any kind or nature. In addition, customers agree not to attempt to gain unauthorized access to other computer systems or attempt to override any security feature of the Services, and not to interfere with another user's use and enjoyment of the Services or otherwise interfere with the proper functioning of the Services. Customers also agree not to solicit passwords or personal identifying information for unintended, commercial or unlawful purposes.

Prospective or current customers who have been known to act improperly or otherwise be involved in fraudulent robocalling will cause their companies to be rejected by CarrierX as a customer and any existing customer relationships could potentially be severed.

Further, CarrierX's TOS requires all customers to comply with the Telephone Consumer Protection Act and its implementing regulations, the Telemarketing Sales Rule, regulations implementing the FCC's national Do-Not-Call registry, and all other rules and regulations governing the sending of telemarketing calls and/or robocalls.

In accordance with FCC rules referenced below, CarrierX only accepts traffic from providers that at a minimum satisfy the following requirements:

- Accepting traffic from domestic Voice Service Providers only if that Voice Service Provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.
- Accepting traffic from Foreign Voice Service Providers or Foreign Intermediate Providers that use NANP resources that pertain to the U.S. in the caller ID field to send voice traffic to residential or business subscribers in the U.S., only if that foreign provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.
- Accepting traffic from Gateway Providers only if that Gateway Provider's filing (a) appears in the RMD, (b) shows that the Gateway Provider has affirmatively submitted the filing, and (c) has not been de-listed pursuant to an enforcement action.
- Accepting traffic from Non-Gateway Intermediate Providers only if that Non-Gateway

Intermediate Provider's filing (a) appears in the RMD, (b) shows that the Non-Gateway Intermediate Provider has affirmatively submitted the filing, and (c) has not been de-listed pursuant to an enforcement action.

CarrierX's Know Your Customer and Upstream Provider Policy and Procedures involve checking the RMD to see if the Provider's filing (a) appropriately appears in the RMD, (b) shows that the Provider has submitted the filing, and (c) has not been de-listed pursuant to an enforcement action.

Telephone Number Validation:

The Company requires the customer to sign an attestation they have the right to use the telephone number and supply a current bill showing the telephone number is active and assigned to them.

Ongoing Robocall Mitigation

CarrierX has various monitoring and reporting systems in place to analyze traffic on its network for suspicious traffic patterns associated with illegal robocalls or other unlawful usage. CarrierX's monitoring systems assess flags and blocks traffic. CarrierX deploys multiple systems to detect potential robocall activity based on statistics such as average call duration, Answer Seize Ratio ("ASR"), and call count carrier/consumer reports. CarrierX is able to identify potential unlawful robocalling through the following means: reports generated by Call Detail Record ("CDR") and pattern trends, fraud information sharing through industry organizations, and third-party notifications and complaints.

If CarrierX detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, CarrierX takes prompt action to identify the party that is using its network to carry these calls and takes appropriate action.

When warranted, CarrierX may also contact the party sending CarrierX the calls (i.e., CarrierX's carrier/provider customer), and request that they work to investigate their customers (e.g., to identify the party sending them the calls, determine whether the calls are unlawful, and then to eliminate the source of the calling). When CarrierX believes it has identified fraudulent activity, it reserves the right to take any action it deems necessary to eliminate the fraudulent activity.

Updating CarrierX's RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(d)(5), (e)(5) and (f)(5), CarrierX will update its submission in the RMD within 10 business days of any change to the applicable information it must provide and update in the RMD.

The Company's RMP continues to develop as the Company and the industry gain expertise and deploy new robocall mitigation strategies and will be supplemented in future updates.