

NetCarrier Telecom, Inc.

Robocall Mitigation Plan

Updated: February 2026

Introduction

NetCarrier Telecom, Inc. ("NetCarrier" or "Company") is fully STIR/SHAKEN compliant and has implemented the Robocall Mitigation Plan described herein in accordance with the requirements of the FCC rules and orders.

NetCarrier is an STI-GA authorized Service Provider registered with the Secure Telephone Identify Policy Administrator (STI-PA) and participates in the Signature-based Handling of Asserted Information Using toKENs (SHAKEN) ecosystem. The Company authenticates its customers following the Robocall Mitigation strategies described herein and based on that authentication, attaches the appropriate attestation level to its customers' outgoing calls.

Robocall Mitigation: Measures to prevent origination of illegal robocalls

Know Your Customer:

NetCarrier has several processes in place to vet its customers, including the following:

NetCarrier provides services exclusively to non-residential subscribers. Customers are required to provide Company name, address, website URL, contact information, President/CEO contact information, Tax ID and/or D&B number, year company was established, and customer officer signature on the customer service agreement. The Company further vets customers by researching their company website and online reviews. NetCarrier also performs credit checks when applicable.

Netcarrier requires customers to provide it with estimates of their usage and denies service to companies that have a history of short-duration calls or that use dialers. The Company provides usage bundles that are sized in accordance with the Customer's estimated usage volumes.

Telephone Number Validation:

The Company requires all end users who request to port numbers to the Company's service to provide a signed Letter of Authorization ("LOA"). Netcarrier also requests invoice copies of services provided by their current service provider and Customer Service Records to confirm the customer's right to use the telephone numbers.

The Company's customers are not authorized to change the published caller ID number on outbound calls.

International Calling

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

Traceback Requests

Netcarrier is committed to and will respond fully within 24 hours to all traceback requests from the FCC, law enforcement agencies, and the Industry Traceback Consortium and will cooperate with these agencies to investigate and stop any illegal robocallers. The Company has signed a contract amendment with Verizon allowing traceback and is requesting membership in the ITG.

The Company has devoted sufficient resources to provide prompt and complete information to traceback requests. The Company's points of contact to handle traceback requests are:

Name	Title	Contact Information
Michael Bilyk	Director of Operations	bilykm@corp.netcarrier.com ; 267-638-3204
Caryn Gerczak	Director of Carrier Relations	gerczakc@corp.netcarrier.com 215-966-3382
Doug Hubler	CTO	doug.hubler@corp.netcarrier.com 617-480-7104

The Company investigates traceback requests by analyzing its call detail records and switch call history. NetCarrier can also determine the IP address from which the calls are originating and can verify that the Caller ID information is correct. The Company can also analyze a customer's calling trends over time to detect unusual call patterns. If suspicious calling activity is found, the Company will notify the customer and the customer's service will be suspended or terminated for violation of the Company's terms and conditions.

Other Robocall Mitigation Practices

In addition to the measures described above, NetCarrier has enforceable terms and conditions and an Acceptable Use Policy within its contracts that define unacceptable and/or fraudulent use of its services and allow the Company to suspend and/or terminate service if a customer violates the terms of the agreement.

NetCarrier routinely monitors its outbound traffic for unusual or suspicious call patterns. It relies on a third-party vendor, Sinch, to authenticate inbound calls. The Company also relies on its third-party vendors to block any inbound calling coming from companies that are not registered in the Robocall Mitigation Database.

