

Communications and Data Solutions, Inc.

Robocall Mitigation Plan v. 2-15-2026

Introduction

This document outlines the reasonable steps and actions taken by Communications and Data Solutions, Inc. ("Communications and Data Solutions") to mitigate and prevent illegal robocalling. Communications and Data Solutions maintains an ongoing commitment to detect, prevent, and eliminate unlawful robocall activity by:

- Pre-qualifying prospective customers
- Monitoring existing customer traffic for patterns indicative of prohibited robocalls
- Cooperating with underlying carriers, industry partners, and regulatory agencies
- Fully complying with all applicable FCC robocall mitigation and STIR/SHAKEN requirements

Communications and Data Solutions, Inc. provides retail point-to-point data services and Voice over Internet Protocol ("VoIP") calling services. All telecommunications services are provided on a resale-only basis.

As a telecommunications reseller, Communications and Data Solutions, Inc. works closely with its underlying voice provider to ensure network integrity and compliance with federal robocall mitigation mandates.

Communications and Data Solutions, Inc. is fully compliant with the FCC's STIR/SHAKEN authentication requirements.

Know Your Underlying Provider

Communications and Data Solutions, Inc. maintains a Master Service Agreement with its upstream voice provider, Sinch. Communications and Data Solutions, Inc. has received written assurances from Sinch confirming that:

- All eligible calls are signed in compliance with the FCC's STIR/SHAKEN requirements
- Sinch complies with all FCC robocall mitigation rules
- Sinch cooperates fully with traceback investigations

Communications and Data Solutions, Inc. and its upstream provider have agreed to work collaboratively and diligently to mitigate illegal robocalls, including full cooperation in response to traceback requests.

Know Your Customer

Communications and Data Solutions, Inc. conducts screening interviews to understand prospective customers' business models and assess any potential risk of involvement in fraudulent robocalling schemes.

Prior to activating service, Communications and Data Solutions, Inc. may conduct:

- Credit checks
- DUNS verification
- Identity and business validation reviews

Communications and Data Solutions, Inc. will not activate services for prospects who:

- Provide anonymous or unverifiable information
- Present inconsistencies or data mismatches
- Refuse to agree to Communications and Data Solutions, Inc.'s Terms of Use,

which strictly prohibit fraudulent or unlawful voice activity

All customers must agree to Communications and Data Solutions, Inc.'s Terms of Use, including explicit prohibitions against illegal robocalling, as a condition of receiving service.

If individuals associated with a prospective or existing customer are known to have engaged in fraudulent robocalling or other improper conduct, Communications and Data Solutions, Inc. may deny service or terminate the business relationship immediately.

Traceback Requests

Communications and Data Solutions, Inc. is committed to responding fully and promptly — within 24 hours — to all traceback requests received from:

- The Federal Communications Commission (FCC)
- Law enforcement agencies
- The Industry Traceback Group (ITG)
- Other authorized regulatory entities

Communications and Data Solutions, Inc. will devote sufficient internal resources to ensure accurate and timely responses.

Traceback Point of Contact

Communications and Data Solutions, Inc. Traceback Support
Support Manager
Phone: 239-561-3849

Upon receipt of a traceback request:

1. A support ticket is opened with Network Operations.
2. The request is escalated to the switch operator and management is notified.
3. Call logs are reviewed and extracted.
4. Origination rules and DID assignment records are verified.

If a traceback investigation identifies a customer as the source of fraudulent robocalls, Communications and Data Solutions, Inc. will:

- Demand immediate explanation and remediation
- Require verification of mitigation measures
- Reject traffic from the offending customer if remediation does not occur
- Terminate service when necessary

Telephone Numbers and Caller ID Authentication

A Telephone Number (“TN”)-based Caller ID identity refers to the originating telephone number included in call signaling to identify the caller.

Subscribers are permitted to use a TN as caller identity only if:

- The TN is directly assigned and managed by Communications and Data Solutions, Inc., or
- The TN is obtained through Communications and Data Solutions, Inc.’s authorized underlying carrier

Telephone numbers may be:

- Allocated directly by Communications and Data Solutions, Inc.
- Ported in with documentation verifying prior ownership

For multi-line systems, Communications and Data Solutions, Inc. and its underlying provider validate that the originating number matches one of the subscriber’s assigned TNs. Calls failing validation may be rejected.

This validation process supports STIR/SHAKEN authentication and ensures secure caller identity verification.

International Calling

Communications and Data Solutions, Inc. is not currently an international voice services provider.

If Communications and Data Solutions, Inc. elects in the future to provide services to international customers utilizing North American Numbering Plan (NANP) resources, enhanced vetting procedures and telephone number validation controls will be implemented in coordination with its underlying carrier.

Call Analytics

As a reseller, Communications and Data Solutions, Inc. relies on its underlying provider and third-party analytics vendors to determine whether originating calls should be blocked or flagged based on call analytics practices.

Internally, Communications and Data Solutions, Inc. monitors traffic to ensure calls originate only from:

- Known customer locations
- Assigned DIDs and TNs
- Authorized network endpoints

Ongoing Robocall Mitigation Efforts

Communications and Data Solutions, Inc. regularly reviews Call Detail Records (CDRs) to detect suspicious calling behavior and patterns.

Indicators monitored include:

- Abnormally high traffic volumes
- Traffic bursts within short timeframes

- Low call completion rates
- Short-duration calls
- Sequential dialing patterns
- Irregular calling spikes

When suspicious activity is detected, Communications and Data Solutions, Inc. will:

- Identify the originating, terminating, or routing party
- Initiate traceback investigations as necessary
- Verify Caller ID authorization
- Confirm Caller ID name consistency
- Block the customer's ability to originate or route calls
- Notify law enforcement when appropriate

Communications and Data Solutions, Inc. is committed to early identification and rapid remediation of potential robocall activity.

Robocall Mitigation Contact

Please direct all inquiries regarding robocall mitigation matters to:

Jeff Reach
Business & VoIP Operations Manager
Communications and Data Solutions, Inc.
5829 Youngquist Road, Suite 1
Fort Myers, FL 33912
Phone: 239-561-3849
Email: Jeff@cadsfl.com