



# Robocall Mitigation Program Description

Prepared for Robocall Mitigation Database filing purposes

|                                          |                                                                                                                           |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Filing Entity</b>                     | e-Coast Computer & Design, LLC                                                                                            |
| <b>Brand / DBA</b>                       | e-Coast Systems                                                                                                           |
| <b>Company Address</b>                   | 1038 Jenkins Rd Unit 101, Charleston, SC 29407                                                                            |
| <b>Company Phone</b>                     | 843-314-3480                                                                                                              |
| <b>Website</b>                           | ecoastsystems.com                                                                                                         |
| <b>Provider Type</b>                     | Voice Service Provider serving end users                                                                                  |
| <b>STIR/SHAKEN Implementation Status</b> | No STIR/SHAKEN Implementation by filing entity                                                                            |
| <b>Upstream SIP/PSTN Provider</b>        | Voxtelesys                                                                                                                |
| <b>Service Description</b>               | Business voice services using 3CX phone system technology and upstream SIP trunking/PSTN services provided by Voxtelesys. |
| <b>Prepared Date</b>                     | May 7, 2026                                                                                                               |

This description is written to address the robocall mitigation program description requirements applicable to a Voice Service Provider under 47 CFR Section 64.6305 and the FCC Robocall Mitigation Database filing instructions.

## 1. Overview

e-Coast Computer & Design, LLC maintains and enforces this Robocall Mitigation Program to prevent, detect, investigate, and stop unlawful robocall traffic that may originate through services provided by the Company. The Company provides business VoIP services only to known business customers and does not market or provide high-volume outbound calling services, lead generation dialer services, robocalling platforms, auto-dialer services, or telemarketing campaign services.

The Company's voice services are provided using 3CX phone system technology and upstream SIP/PSTN services from Voxtelesys. The Company does not directly operate its own STIR/SHAKEN authentication infrastructure, does not maintain its own Secure Telephone Identity Policy Administrator token, and does not maintain its own STIR/SHAKEN certificate. Calls routed to the PSTN through Voxtelesys are subject to Voxtelesys's STIR/SHAKEN signing and call authentication processes.

All calls originated through the Company's voice services are subject to this Robocall Mitigation Program.

## 2. STIR/SHAKEN Implementation Status

The Company has not implemented the STIR/SHAKEN authentication framework on any portion of its own network. The Company relies on Voxtelesys as its upstream SIP/PSTN provider for PSTN call origination and associated STIR/SHAKEN signing where applicable.

The Company lacks direct control over the network infrastructure necessary to independently implement STIR/SHAKEN authentication, including the upstream PSTN origination network, signing platform, SPC token, and STIR/SHAKEN certificate infrastructure. The Company's role is limited to providing, configuring, billing, supporting, and managing business VoIP services for known end-user business customers using 3CX and upstream Voxtelesys services.

### 3. Customer Due Diligence / Know-Your-Customer Procedures

The Company takes reasonable steps to know its customers before activating voice service. The Company provides voice services only to known business customers and does not activate anonymous, prepaid, disposable, or consumer self-service voice accounts.

Before activating service, the Company may collect and review the following information, as applicable:

- Customer legal business name;
- Business address and service location;
- Billing contact and authorized administrative contacts;
- Business phone numbers and requested caller ID numbers;
- Customer website, business records, or other reasonable indicia of legitimate business operations;
- Payment and billing information;
- Authorized users and administrators;
- Intended use of the voice service.

The Company may decline, suspend, or terminate service where customer information cannot be reasonably verified or where the customer's intended use appears inconsistent with lawful business voice service.

The Company prohibits use of its voice services for illegal robocalling, unlawful spoofing, fraudulent calls, scam calls, impersonation, caller ID manipulation, or any activity that violates applicable law, FCC rules, carrier policies, or the Company's acceptable use standards.

### 4. Caller ID and Number Use Controls

The Company takes reasonable steps to reduce unlawful caller ID spoofing and unauthorized caller ID use. Customers may only use outbound caller ID numbers that are assigned to them, controlled by them, or otherwise authorized for their use.

Where practical, the Company configures 3CX and related SIP settings to limit outbound caller ID to numbers assigned to or approved for the customer. The Company does not knowingly permit customers to originate calls using misleading, false, unauthorized, or fraudulent caller ID information.

If the Company becomes aware that a customer is using unauthorized or misleading caller ID information, the Company may require immediate correction, suspend outbound calling, restrict caller ID presentation, or terminate service.

### 5. Reasonable Steps to Avoid Originating Illegal Robocall Traffic

The Company has implemented the following reasonable steps to avoid originating illegal robocall traffic:

- Business-only customer base: The Company provides managed business VoIP services to known business customers and does not provide anonymous or mass-market self-service voice accounts.
- No high-volume robocalling services: The Company does not sell predictive dialer services, auto-dialer services, mass outbound calling platforms, lead-generation dialer services, or telemarketing campaign services.
- Customer vetting before service activation: The Company reviews customer identity, business purpose, contact information, billing information, and intended service use before activation.
- Acceptable use restrictions: Customers are prohibited from using the service for illegal robocalls, scam calls, unlawful spoofing, fraudulent calls, or calls that violate FCC rules or applicable law.
- Caller ID controls: The Company restricts outbound caller ID use to numbers that are assigned to, controlled by, or authorized for the customer.
- Monitoring for suspicious usage: The Company reviews customer traffic and account activity when suspicious patterns are identified, including abnormal call volume, short-duration call bursts, high failure rates, unusual destination patterns, repeated complaints, traceback notices, carrier alerts, or other indicators of unlawful traffic.

- Investigation and escalation: When suspicious traffic is detected or reported, the Company investigates the account, customer, call records, call patterns, and configuration involved.
- Traffic restriction or suspension: The Company may restrict outbound calling, disable international calling, limit call volume, suspend SIP trunks, suspend customer accounts, or terminate service when illegal or suspicious traffic is confirmed or not adequately explained.
- Cooperation with upstream provider: The Company cooperates with Voxtelesys and other relevant service providers to identify, mitigate, and stop suspected illegal traffic.
- Traceback response procedures: The Company maintains procedures to respond to traceback requests within 24 hours and to cooperate with the FCC, law enforcement, and the registered industry traceback consortium.

## 6. Upstream Provider Due Diligence

The Company uses Voxtelesys as its upstream SIP/PSTN provider. The Company selected Voxtelesys because it provides business SIP trunking services and maintains telecom compliance processes, including STIR/SHAKEN signing for calls originating through its service.

The Company's procedures for knowing its upstream provider include:

- Maintaining account and service records with Voxtelesys;
- Confirming that Voxtelesys provides SIP/PSTN origination for the Company's business voice services;
- Confirming that Voxtelesys performs STIR/SHAKEN signing for outbound calls originating through its network, where applicable;
- Cooperating with Voxtelesys regarding suspicious traffic, traceback requests, complaints, caller ID issues, and mitigation actions;
- Reviewing upstream provider notifications or compliance communications when received.

The Company does not knowingly route voice traffic through upstream providers that are not properly authorized to carry such traffic or that are not listed in the FCC Robocall Mitigation Database when listing is required.

## 7. Analytics, Monitoring, and Blocking

The Company does not operate a standalone carrier-scale robocall analytics platform. The Company uses a combination of internal review, system logs, 3CX call records, Voxtelesys portal/reporting tools, carrier notifications, customer account review, complaint review, and upstream provider mitigation processes to identify and respond to suspected illegal robocall traffic.

The Company's analytics and monitoring process may include review of:

- Unusual outbound call volume;
- Sudden increases in call attempts;
- High-volume short-duration calls;
- Repeated unanswered or failed calls;
- International call spikes;
- Calls inconsistent with the customer's normal business profile;
- Repeated calls to similar number ranges;
- Upstream provider alerts;
- Traceback requests;
- Complaints from called parties, carriers, customers, or regulators;
- Caller ID anomalies or unauthorized number use.

The Company currently relies on Voxtelesys for upstream network-level call authentication, carrier-level traffic controls, and any applicable STIR/SHAKEN signing. If the Company uses a third-party analytics vendor in the future, the Company will update its Robocall Mitigation Database filing as required.

## 8. Traceback Response Commitment

The Company commits to respond fully and within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement, and the registered industry traceback consortium. The Company will cooperate with such entities in investigating and stopping illegal robocallers that use, or attempt to use, the Company's service to originate calls.

Upon receipt of a traceback request, the Company will take reasonable steps to:

- Identify the customer account associated with the traffic;
- Review call detail records, SIP trunk records, 3CX records, and available upstream provider information;
- Determine whether the traffic originated from a Company customer or from another source;
- Provide responsive information to the requesting entity within 24 hours;
- Preserve relevant records where appropriate;
- Coordinate with Voxtelesys or other providers as needed;
- Suspend, restrict, or terminate the customer account if illegal traffic is confirmed or reasonably suspected.

## 9. Investigation and Enforcement Procedures

If the Company identifies or receives notice of suspected illegal robocall traffic, the Company will promptly investigate and take appropriate mitigation action. Depending on the circumstances, mitigation actions may include:

- Contacting the customer for explanation and verification;
- Reviewing customer call logs and usage patterns;
- Restricting outbound calling;
- Blocking international or high-risk destinations;
- Limiting call volume;
- Restricting caller ID presentation;
- Suspending affected extensions, trunks, or accounts;
- Coordinating with Voxtelesys to block or trace traffic;
- Terminating service;
- Reporting information to appropriate regulatory, law enforcement, or traceback authorities when required or appropriate.

The Company will not knowingly allow any customer to continue using its service to originate illegal robocalls.

## 10. Recordkeeping

The Company maintains records reasonably necessary to support its robocall mitigation program, which may include:

- Customer identity and contact records;
- Service addresses and billing records;
- Assigned telephone numbers and caller ID records;
- 3CX configuration records;
- Call detail records available to the Company;
- Voxtelesys account and trunk records;
- Traceback requests and responses;

- Abuse complaints and investigation notes;
- Suspension or termination records.

The Company will retain relevant records for a reasonable period consistent with legal, regulatory, contractual, and operational requirements.

## **11. Regulatory / Law Enforcement History Statement**

To the Company's knowledge, e-Coast Computer & Design, LLC, including its principals, ownership, management, directors, and persons in control, has not been the subject of a formal FCC, law enforcement, or regulatory agency action or investigation with findings of actual or suspected wrongdoing for transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or unlawful spoofing, or for a deficient Robocall Mitigation Database certification or mitigation program description.

If this statement becomes inaccurate, the Company will update its Robocall Mitigation Database filing as required.

## **12. Ongoing Review and Updates**

The Company will periodically review this Robocall Mitigation Program and update its procedures as necessary based on changes in FCC rules, upstream provider requirements, customer usage, traceback experience, industry best practices, and the Company's business operations.

The Company will update its Robocall Mitigation Database filing when required to ensure that its certification and mitigation program description remain accurate, complete, and current.

End of Robocall Mitigation Program Description