

# Robocall Mitigation Program Description

ClearConverse Inc.

FRN 0038816559

## 1. Company Overview

ClearConverse Inc. is a United States-based voice service provider that delivers managed VoIP and SMS messaging services directly to end users. ClearConverse serves verified business customers and does not provide wholesale trunking services or operate as an intermediate provider.

ClearConverse maintains direct oversight of its customer accounts, provisioned devices, calling activity, and access to its voice platform. Public switched telephone network origination and termination are obtained through underlying SIP trunking providers.

## 2. STIR/SHAKEN Implementation Status and Exemption

ClearConverse Inc. is a non-facilities-based voice service provider serving end users. ClearConverse obtains PSTN origination and termination services through underlying SIP trunking providers and does not own or control the carrier network infrastructure used to interconnect with the public switched telephone network.

Outbound calls are authenticated by the underlying provider using that provider's STIR/SHAKEN certificate. ClearConverse does not control the provider's STIR/SHAKEN signing infrastructure or make per-call authentication or attestation decisions.

Accordingly, ClearConverse lacks control over the network infrastructure necessary to implement STIR/SHAKEN and claims the applicable exemption from the STIR/SHAKEN implementation requirement.

Notwithstanding this exemption, all calls originated through ClearConverse are subject to the robocall mitigation program described herein.

## 3. Robocall Mitigation Practices

### A. Know Your Customer Procedures

ClearConverse conducts a Know Your Customer review before activating service for a new customer. These procedures are intended to prevent anonymous, unverifiable, fraudulent, or otherwise inappropriate users from obtaining access to ClearConverse voice services.

Procedures include:

- Verification of customer identity, including legal name and physical address.
- Verification of business customers through sources such as Secretary of State records, EIN confirmation, corporate formation documents, and public business listings.
- Review of the customer's intended use of outbound calling services, including expected call volumes, calling patterns, destinations, and caller identification.
- Confirmation that the customer has a legitimate relationship to telephone numbers or caller names requested for outbound caller identification.
- ClearConverse accepts only verified business customers and does not permit anonymous or unverifiable signups.

ClearConverse applies these customer-verification principles to new customers and reviews existing customer information as appropriate when services are renewed, materially changed, or when account activity creates a reason for further review.

### B. Credential Security and Access Control

ClearConverse does not provide SIP credentials directly to end users.

Devices are remotely provisioned by ClearConverse staff or through approved secure automated provisioning systems. Devices that cannot be provisioned securely are considered incompatible and are not permitted to connect to the ClearConverse voice platform.

These controls reduce the risk that SIP credentials can be exposed, shared, resold, or otherwise obtained by unauthorized persons for the purpose of originating unlawful traffic.

### C. Traffic Monitoring and Call Analytics

ClearConverse monitors calling activity across its voice platform using internal operational tools and analytics capabilities available through its underlying service providers.

Monitoring may include:

- Call volume thresholds and sudden volume increases inconsistent with a customer's historical usage.
- Unusually high percentages of short-duration calls.
- Calling patterns indicative of potentially unlawful, abusive, or spoofed traffic.
- Unusual concentration of calls toward particular destinations or high-cost routes.
- Customer or consumer complaints.
- Carrier abuse notifications.
- Traceback requests or referrals from the Federal Communications Commission, law enforcement, or the industry traceback consortium.

ClearConverse currently performs its monitoring through internal systems and analytics capabilities available from its underlying providers and does not rely upon a dedicated third-party call analytics vendor.

If suspicious traffic or account activity is detected, ClearConverse promptly reviews the account and may contact the customer for additional information or an explanation.

Depending upon the circumstances, ClearConverse may block affected traffic, restrict account capabilities, suspend service, or terminate service when necessary to prevent continued unlawful or abusive calling.

#### **4. Know Your Upstream Provider Procedures**

ClearConverse obtains PSTN origination and termination services through established commercial SIP trunking providers with which ClearConverse maintains direct service relationships.

ClearConverse identifies the providers through which its traffic is exchanged and maintains the account and technical information necessary to identify the applicable upstream provider when investigating calling activity, responding to complaints, or participating in a traceback.

ClearConverse does not rely upon unidentified parties to provide PSTN origination or termination services.

ClearConverse cooperates with its underlying providers when investigating suspected unlawful traffic and considers carrier notices, abuse reports, traceback information, and other relevant information when evaluating customer activity.

#### **5. SMS Messaging Controls**

ClearConverse limits SMS services to verified business customers.

ClearConverse monitors messaging activity using non-content operational information, including message volume, throughput, unusual traffic patterns, carrier complaints, and abuse reports.

ClearConverse does not routinely inspect or monitor the content of customer SMS messages as part of its robocall mitigation program.

When suspicious messaging activity is identified through operational information, carrier notification, or an abuse report, ClearConverse may investigate the affected account and take appropriate action consistent with applicable privacy, security, contractual, and legal requirements.

#### **6. Traceback Cooperation**

ClearConverse Inc. will respond fully and within 24 hours to traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium.

ClearConverse will cooperate with those entities in investigating and stopping illegal robocallers that use its service to originate calls.

ClearConverse maintains customer and calling records sufficient to identify the customer account associated with traffic originated through its voice platform and will provide responsive information as legally appropriate during a traceback or investigation.

#### **7. Response to Illegal or Suspicious Traffic**

ClearConverse takes reasonable steps to prevent its services from being used to originate illegal robocalls.

When ClearConverse identifies suspected unlawful traffic, receives a credible complaint or carrier notification, or receives information from the Commission, law enforcement, or the industry traceback consortium indicating potentially unlawful activity, ClearConverse promptly reviews the affected account.

The review may include examination of calling patterns, account history, caller identification information, customer use case, and other non-content operational information relevant to the suspected activity.

ClearConverse may request an explanation or additional documentation from the customer.

When necessary, ClearConverse may block traffic, restrict calling capabilities, suspend service, or terminate the customer relationship in order to stop unlawful or abusive traffic.

## **8. Enforcement History**

ClearConverse Inc. is a newly formed legal entity and was not itself the subject of the prior Federal Communications Commission enforcement action involving the former Clear Converse Corporation. This history is disclosed because the entities share common management and control.

The prior entity was subject to FCC action concerning deficiencies in its Robocall Mitigation Database certification. On August 25, 2025, the FCC Enforcement Bureau issued a final order that included the prior entity and removed its certification from the Robocall Mitigation Database.

The action concerned deficiencies in the prior entity's Robocall Mitigation Database certification and required mitigation-plan information. ClearConverse Inc. is filing a new certification under its own FCC Registration Number and is providing this Robocall Mitigation Program Description in connection with that filing.

## **9. Continuing Compliance**

ClearConverse Inc. will maintain and follow the robocall mitigation practices described in this program.

ClearConverse will review its procedures as its services, network relationships, regulatory obligations, and technical capabilities change and will update its Robocall Mitigation Database certification and mitigation program when required.

ClearConverse will continue taking reasonable steps to prevent illegal robocall traffic from originating through its services, cooperate with the Federal Communications Commission, law enforcement, the industry traceback consortium, and its underlying service providers, and respond fully to qualifying traceback requests within 24 hours.

**Signed,**



**Daniel Harold**

Chief Executive Officer

ClearConverse Inc.