

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Enterprise Sales Software Inc.

Prepared for the Federal Communications Commission Robocall Mitigation Database

Effective Date	October 6, 2026
Version	1.0
Responsible Officer	Robert Magnetico, Chief Executive Officer

1. Purpose and Scope

This Robocall Mitigation Program describes the specific reasonable steps Enterprise Sales Software Inc. (the “Company”) uses to prevent its voice services from being used to originate illegal robocall traffic. The Program applies to voice calls originated by the Company’s customers through the Company’s cloud-based communications and customer relationship management platform and is intended to satisfy the requirements applicable to voice service providers under 47 C.F.R. § 64.6305(a) and § 64.6305(d)(2).

Enterprise Sales Software Inc. serves business customers and individual professionals using communications services for business purposes. The Company permits lawful business calling, including lawful telemarketing where applicable, but prohibits use of the service for unlawful robocalling, fraudulent or misleading caller identification, unlawful prerecorded or artificial-voice calls, harassment, scams, or other activity that violates federal or state law.

2. Service Architecture and STIR/SHAKEN Status

Enterprise Sales Software Inc. is a non-facilities-based voice service provider. The Company controls its application, customer accounts, telephone-number assignments within the platform, call initiation workflows, account restrictions, and customer-level enforcement. It does not own or operate the underlying public switched telephone network (“PSTN”) facilities or the network-layer STIR/SHAKEN signing infrastructure used to deliver calls to the PSTN.

As of the effective date of this Program, Telnyx, LLC is the Company’s primary underlying voice network provider for PSTN connectivity. Telnyx maintains its own Robocall Mitigation Database filing (RMD0001645) and represents that it has implemented STIR/SHAKEN for calls originated on its platform. The Company does not currently possess or use its own STIR/SHAKEN certificate, SPC token, or signing infrastructure.

The Company does not claim a categorical extension under 47 C.F.R. § 64.6304. Rather, consistent with 47 C.F.R. § 64.6305(d)(2)(i), the Company is unable to independently implement STIR/SHAKEN because it lacks control over the network infrastructure at which authentication is technically performed. The underlying carrier controls the relevant session-border, signing, certificate, and PSTN interconnection functions. The Company therefore certifies “No STIR/SHAKEN Implementation” for its own network while maintaining the mitigation measures described in this Program.

If the Company later obtains the technical control and credentials necessary to authenticate calls under its own certificate, or if its STIR/SHAKEN status otherwise changes, the Company will update its RMD filing within the time required by 47 C.F.R. § 64.6305(d)(5).

3. Know-Your-Customer and New/Renewing Customer Controls

The Company takes affirmative, effective measures designed to prevent new and renewing customers from using its service to originate illegal calls, consistent with 47 C.F.R. § 64.1200(n)(4). The Company does not intentionally provide anonymous access to outbound calling functionality. Its customer identification and due-diligence process uses multiple account and business signals, including the following:

- Account identity information, including customer or authorized-user name, business name where applicable, email address, telephone contact information, and account credentials.
- Billing and payment information associated with the customer account, together with account history and other information available through the commercial relationship.
- Business identity information associated with services used by the customer. Where a customer uses 10DLC messaging, the Company also collects or processes business registration information such as legal business name and EIN or other tax/business identifiers as required by the applicable messaging registration process; this information may provide an additional identity signal for the same customer account.

- The customer's intended business use of the platform and other risk indicators reasonably available to the Company. Accounts presenting materially inconsistent, incomplete, suspicious, or high-risk information may be restricted pending additional review or additional proof of identity or business legitimacy.
- Ongoing review after activation. Existing and renewing customers remain subject to complaint review, carrier feedback, usage-pattern review, compliance history, and additional due diligence when circumstances warrant. Continued access is not guaranteed merely because an account previously passed onboarding.

Where the Company identifies a material compliance concern, it may require additional information concerning the customer's identity, business, calling purpose, lead source, consent practices, or authority to use a telephone number before permitting continued calling. The Company may also limit functionality during review.

4. Customer Compliance Requirements and Contractual Controls

The Company requires customers to use the platform only for lawful communications and maintains contractual and policy rights to restrict or terminate service for unlawful or abusive use. The Company's compliance requirements include, as applicable to the customer's calling activity:

- Compliance with the Telephone Consumer Protection Act, the Telemarketing Sales Rule, federal and state do-not-call requirements, caller-ID and spoofing laws, and other applicable communications and consumer-protection laws.
- Obtaining and maintaining any consent, permission, established business relationship, or other legal basis required for the customer's calls, including any additional requirements that apply to artificial or prerecorded voice calls or telemarketing.
- Honoring valid do-not-call, opt-out, consent-revocation, and suppression requests and refraining from intentionally contacting persons whom the customer is legally prohibited from calling.
- Prohibition on fraudulent, deceptive, threatening, harassing, scam-related, or otherwise unlawful calls and on knowingly transmitting misleading or unauthorized caller identification information.
- Cooperation with the Company's compliance inquiries, carrier investigations, traceback requests, and requests for information reasonably necessary to investigate suspected unlawful traffic.

The Company reserves the right to block or restrict traffic, disable telephone numbers or calling functionality, suspend an account, require remediation, or terminate service when the Company has a reasonable basis to believe its services are being used for illegal or abusive calling.

5. Telephone Number and Caller-ID Controls

The Company uses customer-account and telephone-number controls to reduce the risk of spoofing and unauthorized caller-ID presentation. Through the Company's ordinary workflow, outbound caller identification is associated with telephone numbers provisioned to the customer account through the Company's carrier relationship or otherwise verified for authorized use. The Company does not knowingly authorize a customer to present a telephone number that the customer has no right to use.

The Company does not intentionally circumvent network-level call blocking or do-not-originate controls. The Company's application-layer caller-ID controls complement the blocking and validation controls applied by its underlying carrier, including controls applicable to invalid, unallocated, unused, inbound-only, or otherwise inappropriate originating numbers under 47 C.F.R. § 64.1200(o).

6. Call Monitoring, Analytics, Complaints, and Risk Signals

The Company uses first-party application and account information to identify activity that may warrant compliance review. The Company's internal monitoring is based on information reasonably available at the application layer, including call-detail and account records, originating customer/account, calling number, destination information, timestamps, call duration and disposition information, traffic volume, account history, carrier notifications, consumer complaints, and regulatory or traceback requests.

Risk signals that may trigger review include, depending on context, abrupt changes in call volume or destinations, unusually high rates of short-duration or failed calls, evidence that caller identification is invalid or unauthorized, repeated consumer or carrier complaints, known scam indicators, traceback activity, or calling patterns materially inconsistent with the customer's stated or historical use. Because the Company serves legitimate high-volume business users, high call volume by itself is not treated as evidence of unlawful conduct; the Company evaluates the surrounding facts and risk indicators.

The Company does not currently rely on a separate standalone third-party robocall analytics vendor at the application layer. Network-layer STIR/SHAKEN authentication, carrier fraud/abuse controls, and related network analytics are performed by Telnyx, LLC as the underlying network provider. The Company uses carrier feedback and enforcement signals from Telnyx, together with its own account-level information, when investigating suspicious traffic.

7. Investigation, Mitigation, and Enforcement

When the Company receives credible information suggesting that a customer may be originating illegal or abusive traffic, the Company conducts a risk-based review and takes action appropriate to the circumstances. Depending on the severity and reliability of the information, actions may include:

1. Temporarily limiting or suspending outbound calling while the activity is reviewed.
2. Contacting the customer and requiring an explanation, business-use information, proof of identity, authority to use the calling number, consent documentation, lead-source information, or other records relevant to the suspected activity.
3. Blocking identified traffic, telephone numbers, destinations, or calling functionality where appropriate and technically available at the Company's application layer.
4. Coordinating with the underlying carrier and providing information reasonably necessary for carrier or traceback investigation.
5. Requiring corrective action or enhanced controls before service is restored or continued.
6. Suspending or terminating the customer relationship when the Company determines that the customer is using, or presents an unacceptable risk of using, the service for illegal calling or refuses to cooperate with a legitimate compliance investigation.

The Company will not knowingly continue to enable illegal robocalling after credible evidence establishes that a customer is using the service unlawfully. The Company may act before a final governmental determination where available evidence reasonably warrants protective action.

8. Know-Your-Upstream/Network-Provider Procedures

The Company maintains a direct commercial and technical relationship with its underlying voice network provider rather than accepting anonymous wholesale traffic from unknown carriers. As of the effective date, Telnyx, LLC is the Company's primary direct voice-network provider. The Company verifies that its direct network provider is listed in the FCC Robocall Mitigation Database and monitors material carrier or regulatory notices relevant to continued lawful interconnection.

Before placing material voice traffic with any additional network provider, the Company's procedure is to evaluate the provider's identity, RMD status, role in the call path, STIR/SHAKEN status where applicable, contractual terms, and ability to cooperate with traceback and abuse investigations. The Company will not knowingly route traffic through a provider that the FCC requires downstream providers to block or from which the Company is otherwise prohibited from accepting traffic.

For inbound traffic received through the Company's direct network interconnection, the Company relies on the underlying carrier's network-level screening and authentication functions and does not intentionally establish direct traffic relationships with unidentified or unvetted originating providers.

9. Traceback Response and Cooperation

The Company commits to respond fully and within 24 hours to all traceback requests received from the Federal Communications Commission, law enforcement, or the industry traceback consortium, and to cooperate with those entities in investigating and stopping illegal robocallers that use the Company's service to originate calls, consistent with 47 C.F.R. § 64.6305(a)(2) and § 64.6305(d)(2)(iii).

The Company maintains records designed to permit it to identify the customer account associated with originated traffic, including relevant account information and call-detail records maintained in the ordinary course of business. Upon receiving a valid traceback or law-enforcement request, the responsible compliance personnel will promptly identify the relevant customer and traffic, preserve relevant records, provide a complete response within the required timeframe, and take appropriate mitigation action if unlawful use is indicated.

10. Complaint Handling and Escalation

The Company treats credible complaints from consumers, carriers, the FCC, law enforcement, and traceback organizations as compliance signals. Complaints are evaluated together with customer identity, account history, call records, carrier information, and other available facts. Matters indicating potential fraud, spoofing, unlawful prerecorded/artificial-voice calling, repeated unlawful solicitation, or a pattern of noncompliance are escalated for prompt review and possible restriction or termination.

The Company's responsible officer or designated compliance personnel have authority to coordinate investigation and direct account-level mitigation. Urgent carrier, FCC, law-enforcement, and traceback matters receive priority over ordinary support requests.

11. Recordkeeping, Security, and Regulatory Maintenance

The Company maintains account and call-related records in the ordinary course of business for operational, billing, security, dispute-resolution, legal, and compliance purposes. Access to customer and compliance information is limited to personnel or service providers with a business need for such information, and the Company applies administrative and technical security controls appropriate to the information maintained.

The Company reviews this Program periodically and updates its practices when warranted by changes in its services, carrier relationships, identified abuse patterns, or applicable law. The Company will update required RMD information within 10 business days of a reportable change under 47 C.F.R. § 64.6305(d)(5) and will complete the annual RMD recertification on or before March 1 as required by 47 C.F.R. § 64.6305(h).

12. Prior Enforcement Actions / Investigations

For purposes of the Company's current RMD filing, the Company represents that neither the filing entity nor an entity sharing common ownership, management, directors, or control with the filing entity has, during the prior two years, been the subject of a formal Commission, law-enforcement, or regulatory-agency action or investigation with accompanying findings of actual or suspected wrongdoing of the type described in 47 C.F.R. § 64.6305(d)(2)(iv). If that representation changes, the Company will update its RMD filing as required.

13. Responsible Officer and Program Administration

The Company designates Robert Magnetico, Chief Executive Officer, as the responsible officer for oversight of this Robocall Mitigation Program and for ensuring that appropriate personnel respond to regulatory, carrier, and traceback matters. The Company may delegate day-to-day investigation, support, security, and carrier-coordination tasks while retaining officer-level responsibility for the Program.

Robert Magnetico

Chief Executive Officer

Enterprise Sales Software Inc.

References

- 47 C.F.R. § 64.6305(a), (d), and (h) - Robocall mitigation and certification requirements for voice service providers.
- 47 C.F.R. § 64.1200(n)(4) - affirmative, effective measures to prevent new and renewing customers from originating illegal calls; know-your-customer due diligence.
- 47 C.F.R. § 64.1200(o) - reasonable do-not-originate blocking requirement.
- Call Authentication Trust Anchor, Sixth Report and Order, FCC 23-18 (2023), including the requirement that mitigation plans describe new/renewing customer controls, upstream-provider procedures, contractual provisions, and analytics systems.
- Call Authentication Trust Anchor, Eighth Report and Order, FCC 24-120 (2024), regarding third-party STIR/SHAKEN authentication and provider responsibility for certificates where an implementation obligation applies.
- Wireline Competition Bureau, DA 24-73 (Jan. 25, 2024), Robocall Mitigation Database filing deadlines and instructions.