

Carrier One Robocall Mitigation Program Policy Updated as of February 25, 2026

Commitment to Robocall Mitigation Compliance Carrier One Inc. recognizes the critical importance of protecting consumers, enterprise customers, and the telecommunications ecosystem from illegal and unwanted robocalls. We are committed to full compliance with all Federal Communications Commission (FCC) robocall mitigation, caller authentication, traceback, and database filing requirements, including all rules in effect as of 2026.

Carrier One Inc. maintains a comprehensive robocall mitigation program designed to detect, prevent, investigate, and remediate illegal robocall traffic across our network. We actively collaborate with regulators, industry partners, and traceback organizations to ensure the integrity of voice communications.

Carrier One Inc. does not accept any foreign-originated traffic and does not operate as a Gateway Provider. We do not directly or indirectly receive voice traffic from international carriers for origination into the United States.

1. **Network-Level Robocall Detection** Carrier One Inc. employs advanced technologies and analytic methodologies to identify suspicious calling behavior, including but not limited to:
 - Call Signature Analysis – Monitoring traffic for abnormal patterns such as high-volume bursts, short-duration calls, and repetitive dialing sequences.
 - Real-Time Network Monitoring – 24/7 surveillance of call traffic across switching infrastructure.
 - Snowshoe Dialing Detection – Identification of traffic distributed across large ANI ranges.
 - Neighbor Spoofing Detection – Identification of local spoofing patterns designed to increase answer rates.
 - Invalid Number Blocking – Blocking calls originating from unallocated, invalid, or unassigned numbering resources.
 - Reassigned Number Monitoring – Review of traffic against reassigned number databases where applicable.
 - Scam Pattern Recognition – Detection of known scam campaigns including government impersonation, warranty scams, and financial fraud robocalls.
2. **Robocall Prevention & Removal** Carrier One Inc. takes immediate mitigation action upon detection of suspicious traffic:
 - Automated Call Blocking at the point of detection.
 - Traffic Quarantine for forensic investigation.

- Dynamic Do-Not-Originate (DNO) Enforcement including FCC and internal enterprise DNO lists.
- Spam Scoring & Analytics leveraging industry reputation databases.
- Toll-Free DNO Protections where applicable.

If traffic is confirmed to be illegal or non-compliant, immediate suspension actions are taken.

3. **Know-Your-Customer (KYC) & Customer Vetting Program** Carrier One Inc. maintains a robust wholesale customer onboarding and verification framework to prevent bad actors from accessing our network. As a wholesale-focused provider, all interconnected carriers, resellers, and enterprise wholesale clients are subject to enhanced due diligence prior to service activation.

Customer Identity Verification We collect and verify:

- Legal business name
- Articles of incorporation / formation
- Employer Identification Number (EIN)
- Physical business address
- Responsible corporate officers
- Government-issued identification where appropriate

Traffic Use Case Review We evaluate:

- Intended call types and campaigns
- Dialing methodologies
- Target geographies
- Consent acquisition processes

Contractual Safeguards All customers agree to:

- Prohibitions on illegal robocalling
- TCPA compliance requirements
- STIR/SHAKEN authentication cooperation
- Immediate mitigation obligations

Carrier One Inc. reserves the right to deny or terminate service based on risk assessment.

4. **Per-Customer Traffic Monitoring** Carrier One Inc. continuously monitors customer traffic using:

- Volume baselining
- Answer Seizure Ratio (ASR) analysis
- Average Call Duration (ACD) monitoring
- A-Number spoofing detection
- Call velocity thresholds
- Complaint correlation tracking

Traffic exceeding risk thresholds is subject to immediate review and mitigation.

5. **STIR/SHAKEN Caller Authentication** Carrier One Inc. fully complies with FCC caller authentication mandates.

Call Signing Practices

- We sign all eligible outbound calls.
- We authenticate wholesale customer identity prior to assigning attestation.
- Calls are signed under Carrier One Inc. OCN 705J.

Attestation Governance Carrier One Inc. assigns attestation levels as follows:

- Full Attestation (A): Applied where Carrier One has a direct wholesale relationship and verified right-to-use authorization for the telephone numbers presented.
- Partial Attestation (B): Applied where the wholesale customer relationship is established but number control verification is limited.
- Gateway Attestation (C): Rarely applicable as Carrier One Inc. does not accept foreign-originated traffic.

Carrier One Inc. does not maintain its own retail DID number pools and relies on customer-provided or hosted numbering resources subject to verification.

Additional Controls

- Unique call identifiers (UUIDs)
- Secure SIP identity header management

- Traceability mapping to trunk groups
6. **Traceback Cooperation (ITG)** Carrier One Inc. fully cooperates with the FCC-designated Industry Traceback Group (ITG).

Upon receipt of a traceback request, we:

- Respond within 24 hours (typically within 4 hours)
- Investigate call origin and routing
- Identify responsible customers or upstream providers
- Implement remediation, including blocking or termination

We maintain readiness to participate in all traceback initiatives.

7. **Complaint Intake & Investigation** Carrier One Inc. maintains procedures for receiving and addressing robocall complaints.

Intake Sources

- FCC complaints
- ITG referrals
- Enterprise customer reports
- Direct consumer submissions via email: legal@carrierone.com

Investigation Process

- Call record analysis
- Traffic pattern review
- Customer outreach
- Campaign suspension where warranted

All substantiated violations result in mitigation action consistent with Carrier One Inc. enforcement policies.

8. **Enforcement & Suspension Policy** Carrier One Inc. enforces strict enforcement standards for illegal robocalling.

We reserve the right to:

- Suspend or restrict traffic
- Block originating numbers

- Terminate service agreements
- Report violations to regulators
- Cooperate with law enforcement

Enforcement actions may be taken based on risk severity, investigation findings, and regulatory obligations. Suspension or termination may occur where warranted. This applies to customers, resellers, and interconnected carriers.

9. **Record Retention & Documentation** Carrier One Inc. maintains detailed records to support mitigation and traceback obligations.

Retained Records

- Call Detail Records (CDRs)
- SIP signaling data
- Customer onboarding documentation
- Traceback responses
- Complaint investigations

Retention Periods Records are retained for a minimum of 24 months or longer where required by regulation or enforcement activity.

10. **Regulatory Filings & Database Compliance** Carrier One Inc. maintains full compliance with FCC administrative requirements, including:
 - Active filing in the Robocall Mitigation Database (RMD), detailing our robocall mitigation plan, STIR/SHAKEN implementation status, and related certifications.
 - **Annual recertification** of our RMD filing on or before **March 1** each year. The first recertification is required by **March 1, 2026** (filing window opens February 1, 2026). Recertification involves logging into the RMD portal (using multi-factor authentication as required effective February 5, 2026), reviewing/verifying all information for accuracy (including mitigation practices, STIR/SHAKEN certifications, and contacts), making updates if needed, and submitting via the "Recertify" button.
 - **Prompt updates** to our RMD filing within **10 business days** of any material change (e.g., ownership, control, contact information, or operational details), per 47 CFR § 64.6305.
 - Timely updates to our CORES registration information within **10 business days** of any change, effective February 5, 2026.

- Prompt responses to any FCC notices regarding deficient or inaccurate filings.
- Payment of any required filing fees when effective (note: the \$100 application fee for initial and annual recertifications, adopted in the 2025 Robocall Mitigation Database Report and Order, is not yet in effect and was not required for the 2026 recertification; FCC will announce when effective).

Failure to comply may result in FCC enforcement actions, including base forfeitures of \$10,000 for submitting false or inaccurate information and \$1,000 (per day until cured) for failure to update within 10 business days, potential removal from the RMD, and downstream blocking of traffic.

11. Emerging Threat Mitigation Carrier One Inc. monitors evolving robocall threat vectors, including:

- AI-generated voice campaigns
- Voice cloning fraud
- Prerecorded message fingerprinting
- Synthetic identity call campaigns

We continue to invest in analytic and detection technologies to address emerging risks.

12. Continuous Program Governance Our robocall mitigation framework is continuously updated to reflect:

- FCC rulemakings
- Enforcement advisories
- Industry best practices
- STIR/SHAKEN standards evolution

Carrier One Inc. remains committed to protecting the public and maintaining the highest standards of telecommunications compliance.

Authorized By: Carrier One Inc. Compliance Department

Contact: Regulatory Compliance Officer

Program Review Cycle: Annual or as required by FCC rule changes