

ROBOCALL MITIGATION PLAN

Constellate Group LLC

Filed Pursuant to 47 CFR § 64.6305

Last Updated: February 6, 2026

IMPORTANT NOTICE REGARDING CURRENT STATUS

Constellate Group LLC is not currently selling, offering, or providing any telecommunications services. Constellate Group LLC has no customers, no end users, and does not originate, carry, or terminate any voice traffic at this time.

Constellate Group LLC is a research-stage organization conducting development research related to a potential project involving the Public Switched Telephone Network (PSTN). The organization is not an operating telecommunications company.

This filing is submitted in the Robocall Mitigation Database in anticipation of future activities and to ensure regulatory compliance during the research phase. Should circumstances change—including any commencement of service offerings or customer acquisition—Constellate Group LLC will immediately notify the Federal Communications Commission and update this plan accordingly.

I. Purpose and Scope

This Robocall Mitigation Plan (“Plan”) is submitted by Constellate Group LLC (“Constellate” or the “Company”) pursuant to 47 CFR § 64.6305, as required by the Federal Communications Commission (“FCC”). This Plan is filed in the Robocall Mitigation Database (“RMD”) to demonstrate Constellate’s commitment to compliance with federal robocall mitigation requirements.

Constellate Group LLC is currently in a research and development phase, exploring a potential project related to the Public Switched Telephone Network (PSTN). **At this time, Constellate does not sell, offer, or provide any telecommunications services. Constellate has no customers, no end users, and does not originate, carry, process, or terminate any voice traffic.**

Because Constellate is not currently operating as a voice service provider and does not handle any call traffic, the risk of originating, carrying, or processing illegal robocall traffic is nonexistent at this time. Nonetheless, Constellate submits this Plan in good faith and in anticipation of potential future operations.

II. Current Operational Status

- **Business Status:** Research-stage organization; not an operating telecommunications company.
- **Customer Base:** None. Constellate has no customers, subscribers, or end users.
- **Voice Traffic:** Constellate does not originate, carry, process, or terminate any voice calls.
- **Network Infrastructure:** Constellate does not currently operate any telecommunications network infrastructure.
- **STIR/SHAKEN Status:** Not applicable at this time. Constellate does not control network infrastructure and does not handle any IP or TDM voice traffic. Implementation will be addressed if and when operations commence.

III. Commitment to Regulatory Compliance

Constellate Group LLC is committed to full compliance with all applicable FCC regulations, including but not limited to:

- The Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227
- The Truth in Caller ID Act, 47 U.S.C. § 227(e)
- FCC rules regarding STIR/SHAKEN implementation and caller ID authentication (47 CFR §§ 64.6300–64.6308)
- FCC rules regarding robocall mitigation and certification (47 CFR § 64.6305)
- All applicable state-level robocall and telemarketing regulations
- The January 2026 Report and Order strengthening RMD requirements, including annual recertification by March 1 and the obligation to update filings within ten business days of any material change

IV. Traceback Commitment

Constellate Group LLC commits to responding within 24 hours to all traceback requests from the FCC, law enforcement agencies, and the Industry Traceback Group (ITG), and to cooperating fully with such entities in investigating and stopping any illegal robocallers, in accordance with 47 CFR § 64.6305.

As Constellate does not currently originate, carry, or terminate any voice traffic, no traceback requests are anticipated at this time. However, this commitment is in place and will be fully operational if and when Constellate commences providing services.

V. Current Robocall Mitigation Measures

Given that Constellate Group LLC does not currently originate, carry, process, or terminate any voice traffic, the following measures constitute the Company's current robocall mitigation program:

1. **No Voice Traffic:** Constellate does not handle any voice calls, eliminating the possibility of originating or transmitting illegal robocalls.
2. **No Customer Relationships:** Constellate has no customers or end users who could use its services for robocalling purposes.
3. **No Network Access:** Constellate does not provide access to any telecommunications network that could be exploited for illegal robocalling.
4. **Monitoring Commitment:** Constellate actively monitors regulatory developments to ensure that its Plan remains current and will be updated as circumstances change.
5. **Future Operational Plan:** Constellate has prepared a comprehensive Robocall Mitigation Plan (attached as Exhibit A) that will be activated upon commencement of service operations.

VI. Notification and Update Obligations

Constellate Group LLC commits to the following notification and update obligations:

- **Immediate Notification to the FCC:** Constellate will immediately notify the FCC and update this Plan, its RMD certification, and all related filings in the event of any material change in its operational status, including but not limited to: commencement of any telecommunications service offerings, acquisition of any customers or end users, origination, carrying, processing, or termination of any voice traffic, or deployment of any telecommunications network infrastructure.
- **Ten-Business-Day Update Obligation:** Consistent with the January 2026 Report and Order, Constellate will update its RMD filing within ten (10) business days of any material change to the information contained therein.
- **Annual Recertification:** Constellate will recertify its RMD filing by March 1 of each year, as required by the FCC.
- **Plan Activation:** Upon commencement of operations, Constellate will immediately activate the comprehensive Robocall Mitigation Plan set forth in Exhibit A (or an updated version thereof reflecting the Company's actual operational configuration at that time).

VII. Enforcement and Investigations Disclosure

Constellate Group LLC certifies that neither it nor any affiliated entity has, at any time in 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 related to the transmission, encouragement, assistance, or facilitation of illegal robocalls or caller ID spoofing.

VIII. Review and Approval

This Plan has been reviewed and approved by the executive management of Constellate Group LLC. It will be subject to periodic review to ensure its ongoing relevance, effectiveness, and compliance with applicable FCC regulations.

This Plan was last updated on February 6, 2026.

A handwritten signature in black ink, appearing to be 'CIB', is written over a horizontal line.

Authorized Officer, Constellate Group LLC

Date: February 6, 2026

EXHIBIT A

Comprehensive Robocall Mitigation Plan

Constellate Group LLC

To Be Activated Upon Commencement of Service Operations

NOTE: This Exhibit sets forth the comprehensive Robocall Mitigation Plan that Constellate Group LLC will implement if and when its research concludes and the Company begins offering telecommunications services. This plan is provided to demonstrate that Constellate has proactively developed robust policies, procedures, and controls to prevent the origination, carrying, and processing of illegal robocall traffic. This Exhibit will be updated as necessary to reflect Constellate's actual operational configuration at the time of service commencement and will replace the research-phase plan in the main body of this filing at that time.

1. Introduction and Purpose

This Comprehensive Robocall Mitigation Plan ("Operational Plan") establishes the policies, procedures, technical controls, and organizational commitments that Constellate Group LLC will implement upon commencement of telecommunications service operations. The Operational Plan is designed to ensure that Constellate takes all reasonable steps to avoid originating, carrying, or processing illegal robocall traffic, in compliance with 47 CFR § 64.6305 and all related FCC requirements.

This Plan covers all aspects of robocall mitigation, including: Know Your Customer (KYC) practices, STIR/SHAKEN implementation, call traffic monitoring and analytics, enforcement and penalties, traceback cooperation, customer education, incident response, documentation, regulatory compliance, and ongoing review.

2. Know Your Customer (KYC) Program

2.1 Customer Onboarding and Vetting

Before providing service to any customer, Constellate will perform comprehensive due diligence to verify the identity, legitimacy, and intended use of its services:

- **Identity Verification:** Collect and verify the customer's legal business name, principal business address, state of incorporation or registration, Employer Identification Number (EIN) or equivalent, and the identity of authorized representatives.
- **Business Legitimacy Screening:** Verify the customer's business registration with the relevant Secretary of State, confirm active good standing, and conduct

screening against the FCC's enforcement action records, the FTC's Do Not Call complaint database, and relevant industry blacklists.

- **Use Case Assessment:** Require each customer to provide a detailed description of its intended use of Constellate's services, including expected call volumes, types of calls (transactional, informational, marketing), and target audiences.
- **Acceptable Use Policy (AUP) Agreement:** Require all customers to execute a binding Acceptable Use Policy that expressly prohibits the origination of illegal robocalls, caller ID spoofing, and any use of Constellate's services in violation of the TCPA, Truth in Caller ID Act, or any applicable state or federal law.
- **Reference and Background Checks:** For high-volume customers or those in industries commonly associated with robocalling (e.g., debt collection, telemarketing, lead generation), conduct enhanced due diligence including reference checks, review of prior regulatory history, and verification of required licenses or registrations.

2.2 Ongoing Customer Monitoring

- **Periodic Re-Verification:** Re-verify customer information at least annually, or more frequently for high-risk customers.
- **Traffic Pattern Analysis:** Continuously monitor customer call traffic for anomalies, including sudden spikes in call volume, high rates of short-duration calls, calls to known honeypot numbers, and unusual geographic distribution patterns.
- **Complaint Monitoring:** Track and investigate all complaints received regarding a customer's call traffic, including complaints from other carriers, the FCC, state regulators, and end users.
- **Watchlist Screening:** Regularly screen customers against updated FCC enforcement action lists, ITG traceback data, and industry robocall databases.

3. STIR/SHAKEN Implementation

3.1 Call Authentication Framework

Upon commencement of operations, Constellate will implement the STIR/SHAKEN caller ID authentication framework on all IP portions of its network, in compliance with 47 CFR §§ 64.6300–64.6308:

- **SPC Token and Certificate:** Obtain a Service Provider Code (SPC) token and digital certificate from the STI Policy Administrator (STI-PA) and STI Certificate Authority (STI-CA).

- **Attestation Levels:** Apply the appropriate attestation level (Full Attestation “A,” Partial Attestation “B,” or Gateway Attestation “C”) to all outbound calls, based on the Company’s knowledge of the calling party and origination point.
- **Own-Certificate Signing:** In accordance with the September 2025 third-party authentication rules, Constellate will use its own certificate and make its own attestation decisions for all calls, even if utilizing a third-party authentication platform.
- **Verification on Termination:** Implement STIR/SHAKEN verification on all incoming calls on IP segments of the network to validate caller ID information before delivering calls to end users.

3.2 Caller ID Management

- **Caller ID Accuracy:** Ensure that all caller ID information transmitted from Constellate’s network is accurate and properly reflects the calling party’s identity.
- **Spoofing Prevention:** Implement technical controls to prevent customers from transmitting false or misleading caller ID information in violation of the Truth in Caller ID Act.
- **Number Validation:** Validate that customers have authorization to use the calling numbers they present, including verification against number assignment records and carrier-of-record databases.

4. Robocall Detection and Prevention

4.1 Advanced Analytics and Monitoring

- **Real-Time Traffic Analysis:** Deploy real-time analytics tools to monitor all call traffic for patterns indicative of illegal robocalling, including high call volumes from single sources, short-duration call patterns, calls to known Do Not Call registrants, and rapid-fire sequential dialing.
- **Machine Learning Models:** Utilize machine learning algorithms trained on known robocall patterns to identify and flag suspicious traffic in real time.
- **Network Monitoring:** Continuously monitor network infrastructure for unusual traffic patterns, unauthorized access attempts, and signs of network compromise that could facilitate robocalling.
- **Honeypot Integration:** Participate in industry honeypot programs to identify callers that are dialing unassigned or known-trap numbers, a strong indicator of illegal robocalling.

4.2 Call Blocking and Traffic Management

- **Mandatory Blocking Compliance:** Comply with all FCC mandatory call blocking rules, including blocking calls from providers not listed in the RMD, calls from

numbers on the DNO (Do Not Originate) list, and calls identified through reasonable analytics as likely illegal.

- **Permissive Blocking:** Implement permissive call blocking based on reasonable analytics, including blocking calls from numbers that are invalid, unallocated, or unused, and calls matching known robocall signatures.
- **RMD Verification:** Before accepting traffic from any upstream provider, verify that the provider has a valid, active filing in the Robocall Mitigation Database that has not been de-listed pursuant to FCC enforcement action.
- **Rate Limiting:** Implement rate-limiting controls to prevent any single customer or source from generating call volumes inconsistent with their stated use case and contracted capacity.

5. Enforcement, Penalties, and Customer Accountability

5.1 Acceptable Use Policy Enforcement

Constellate will enforce its Acceptable Use Policy through a graduated enforcement framework:

1. **First Violation (Minor):** Written warning with requirement to cure the violation within 24 hours. Customer's account flagged for enhanced monitoring.
2. **Second Violation or Failure to Cure:** Temporary suspension of service pending investigation. Customer required to demonstrate corrective action before service is restored.
3. **Serious or Repeated Violations:** Immediate suspension and potential permanent termination of service. Referral to the FCC, law enforcement, and the Industry Traceback Group as appropriate.
4. **Confirmed Illegal Robocalling:** Immediate and permanent termination of service. Full cooperation with FCC and law enforcement investigations. Reporting to relevant industry databases and traceback entities.

5.2 Internal Compliance

- **Employee Training:** All employees and contractors involved in network operations, customer onboarding, or traffic management will receive regular training on robocall identification, mitigation procedures, and regulatory requirements.
- **Internal Auditing:** The compliance team will conduct regular internal audits of robocall mitigation practices, customer vetting procedures, and traffic monitoring effectiveness.

- **Whistleblower Protections:** Establish a confidential reporting mechanism for employees to report suspected violations of the Company's anti-robocall policies without fear of retaliation.

6. Traceback Cooperation and Law Enforcement Coordination

- **24-Hour Response Commitment:** Constellate will respond within 24 hours to all traceback requests from the FCC, law enforcement agencies, and the Industry Traceback Group (ITG), in compliance with 47 CFR § 64.6305.
- **Designated Traceback Contact:** Maintain a designated point of contact for all traceback inquiries, available during and outside of normal business hours.
- **Investigation Cooperation:** Cooperate fully with the FCC, ITG, state regulators, and law enforcement in investigating the source and path of suspected illegal robocall traffic.
- **Call Detail Record Retention:** Retain call detail records (CDRs) for a sufficient period to support traceback investigations and regulatory compliance, in accordance with applicable retention requirements.
- **Industry Collaboration:** Actively participate in industry working groups, information-sharing initiatives, and cooperative efforts to combat illegal robocalling, including collaboration with the ITG, USTelecom, and other relevant bodies.

7. Customer Education and Support

- **Educational Materials:** Provide customers with educational materials regarding illegal robocalls, including how to recognize them, how to report them, and the legal consequences of originating or facilitating them.
- **AUP Communication:** Clearly communicate the Company's Acceptable Use Policy, including prohibited activities and the consequences of violations, to all customers at onboarding and on an ongoing basis.
- **Customer Support:** Maintain a dedicated support channel for customers to report robocall-related issues, ask compliance questions, and receive guidance on lawful calling practices.
- **Regulatory Updates:** Proactively notify customers of relevant regulatory changes that may affect their calling practices or compliance obligations.

8. Incident Response and Recovery

8.1 Incident Response Team

Constellate will establish a dedicated Robocall Incident Response Team (“RIRT”) responsible for:

- Receiving and triaging reports of suspected illegal robocall activity on the Company’s network
- Coordinating the Company’s response to traceback requests and regulatory inquiries
- Investigating and resolving incidents, including identifying the source, scope, and impact of suspected illegal traffic
- Implementing containment measures, including emergency traffic blocking, customer suspension, and network isolation
- Communicating with affected parties, including other carriers, regulators, and law enforcement

8.2 Recovery Procedures

- **Root Cause Analysis:** Conduct a thorough root cause analysis following every significant incident to identify how the illegal traffic entered or transited the network.
- **Corrective Action:** Implement corrective actions to prevent recurrence, including updated monitoring rules, enhanced customer vetting, or network configuration changes.
- **Post-Incident Review:** Conduct a post-incident review within 30 days of each significant incident, documenting findings, actions taken, and lessons learned.

9. Documentation and Reporting

- **Comprehensive Records:** Maintain detailed records of all robocall mitigation activities, including customer vetting records, traffic monitoring reports, traceback responses, incident reports, enforcement actions, audit findings, and training records.
- **Regulatory Reporting:** Ensure timely and accurate reporting to the FCC and other regulatory bodies as required, including annual RMD recertification, filing updates within ten business days of material changes, and any required breach or incident notifications.
- **Record Retention:** Retain all records related to robocall mitigation for a minimum of five (5) years, or such longer period as required by applicable law or regulation.
- **Management Reporting:** Provide regular reports to executive management summarizing robocall mitigation activities, incidents, enforcement actions, audit results, and regulatory developments.

10. Audits and Continuous Improvement

- **Quarterly Reviews:** Conduct quarterly reviews of traffic monitoring data, customer vetting effectiveness, and incident response outcomes.
- **Annual Comprehensive Audit:** Perform an annual comprehensive audit of all elements of this Robocall Mitigation Plan, including KYC procedures, STIR/SHAKEN implementation, detection and prevention tools, enforcement practices, and documentation.
- **Regulatory Update Review:** Review and incorporate new FCC guidance, enforcement actions, and regulatory changes within 30 days of publication.
- **Technology Assessment:** Regularly evaluate and adopt new technologies and industry best practices for robocall detection, prevention, and mitigation.
- **Third-Party Assessment:** Consider engaging an independent third party to periodically assess the effectiveness of the Company's robocall mitigation program.

11. Implementation Timeline

The following timeline will be executed upon commencement of service operations (Day 1 = first day of service):

Timeframe	Actions
Pre-Launch	Complete STIR/SHAKEN certification (SPC token, digital certificate); finalize KYC onboarding procedures; deploy traffic monitoring and analytics tools; train all relevant staff; update RMD filing to reflect operational status
Day 1–30	Activate all monitoring and detection systems; begin customer onboarding under full KYC protocols; begin STIR/SHAKEN signing of all outbound calls; establish RIRT availability
Days 31–90	Conduct first quarterly review of traffic data and customer vetting; refine analytics thresholds and monitoring rules; complete first internal audit cycle
Days 91–180	Deploy enhanced analytics and machine learning models; establish full industry collaboration and ITG integration; conduct first comprehensive incident response drill
Days 181–365	Complete first annual comprehensive audit; evaluate third-party assessment engagement; refine all procedures based on operational experience; prepare for first annual RMD recertification
Ongoing	Continuous monitoring, quarterly reviews, annual audits, annual RMD recertification by March 1, filing updates within 10 business days of material changes

12. Regulatory Framework Reference

This Operational Plan is designed to comply with the following regulatory requirements, among others:

- Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227
- Truth in Caller ID Act, 47 U.S.C. § 227(e)
- STIR/SHAKEN Implementation Rules, 47 CFR §§ 64.6300–64.6308
- Robocall Mitigation and Certification, 47 CFR § 64.6305
- FCC Report and Order on Improving the Effectiveness of the Robocall Mitigation Database (January 2026)
- FCC Eighth Report and Order on Third-Party STIR/SHAKEN Authentication (November 2024, effective September 2025)
- All applicable state robocall and telemarketing regulations

--- End of Exhibit A ---