

Robocall Mitigation Plan

Service Offering: CyberShield VoIP

Date of Filing/Update: March 1, 2026

I. Introduction and Commitment

CyberShield Technology Solutions LLC ("CyberShield") is a voice service provider (VSP) dedicated to the prevention of illegal robocalls. We certify that we have implemented a Robocall Mitigation Plan to ensure that CyberShield does not originate illegal robocall traffic. As of March 1, 2026, CyberShield is in compliance with the FCC's annual recertification requirements and maintains its information in the Robocall Mitigation Database (RMD).

II. Specific Mitigation Steps (Reasonable Steps)

CyberShield takes the following specific, reasonable steps to avoid originating illegal robocall traffic:

1. **Know Your Customer (KYC):** We perform identity verification for all new business and residential subscribers. This includes verifying the physical address, tax ID (for businesses), and valid contact information. We cross-reference applicants against known high-risk lists.
2. **Vetting Caller Identity:** We follow the best practices described by the NANC Call Authentication Trust Anchor Working Group to ensure that our users are who they claim to be.
3. **Wholesale Partnership:** CyberShield utilizes Atheral LLC (FRN 0028070290) for origination, termination, and hosted-switch access. We rely on Atheral's industry-leading STIR/SHAKEN implementation and real-time monitoring tools to supplement our internal mitigation efforts.

III. Acceptable Use Policy (AUP) & Enforcement

All CyberShield VoIP subscribers are bound by an AUP that strictly prohibits:

1. Using the service for fraudulent or deceptive activities.
2. Originating "robocalls" that violate the TCPA or TRACED Act.
3. Spoofing caller ID information with the intent to defraud or cause harm.
4. Engaging in "traffic pumping" or "Wangiri" schemes.

Enforcement: CyberShield maintains a "Zero Tolerance" policy. If suspicious activity is detected, we reserve the right to suspend or terminate service immediately.

IV. Commitment to Traceback and Cooperation

CyberShield is fully committed to the industry-wide effort to stop illegal calls:

1. Traceback Response: We respond to all traceback requests from the FCC, law enforcement, state attorneys general, and the Industry Traceback Group (ITG) within 24 hours.
2. Point of Contact: Traceback requests should be sent to noc@cybershieldms.com for immediate processing.
3. Customer Cooperation: Our AUP mandates that subscribers cooperate with any investigation into call patterns. Failure to comply results in immediate account suspension.

V. Real-Time Monitoring and Analytics

Through our partnership with Atheral LLC, we utilize TransNexus's ClearIP solution to monitor our outbound traffic in real-time. We specifically monitor for:

1. High-Volume Triggers: Unusual spikes in outbound call volume compared to historical benchmarks.
2. Short Duration Calls (SDC): Excessive percentages of calls lasting less than 6 seconds (a primary indicator of robocalling).
3. Invalid Caller IDs: Blocking calls from unallocated, unassigned, or "Do Not Originate" (DNO) numbers.
4. Reputation Filtering: Monitoring calls against the FCC consumer complaint

database.

VI. STIR/SHAKEN Implementation Status

CyberShield, through its partnership with Atheral LLC, has fully implemented the STIR/SHAKEN framework on all IP portions of its network.

Attestation: Calls originated by CyberShield customers are signed by our upstream provider (Atheral) using the highest level of attestation possible based on the verified relationship with the subscriber.

Certification: We certify that we have implemented STIR/SHAKEN on all SIP-based traffic.