

SRWS NETWORKS LLC

Robocall Mitigation Plan

Entity Snapshot

- **Company Name:** SRWS NETWORKS LLC
- **Business Type:** U.S.-Based Domestic Wholesale Telecommunications Provider
- **Principal Business Address:** 1001 S. Main Street, Ste 600, Kalispell, MT 59901
- **Business Phone:** 406-476-4030
- **Federal Employer Identification Number (EIN):** 61-2278178
- **FCC Registration Number (FRN):** 0038372579
- **Robocall Mitigation Database (RMD) Filing ID:** RMD0040045
- **Additional Regulatory Reference No.:** 838955471M

This Robocall Mitigation Plan (RMP) describes the policies, technical controls, operational procedures, and enforcement measures implemented by SRWS NETWORKS LLC to detect, prevent, and mitigate illegal robocalls in full compliance with 47 CFR § 64.6305 and the FCC's Robocall Mitigation Database filing requirements. SRWS NETWORKS LLC operates as a U.S.-based domestic wholesale telecommunications provider and applies STIR/SHAKEN call authentication with Attestations A, B, and C as appropriate to the traffic it originates and carries.

1. Entity Information & Commitments

- **Company Name:** SRWS NETWORKS LLC
- **Business Type:** U.S.-based Domestic Wholesale Telecommunications Provider
- **Regulatory Compliance:** Fully FCC registered, compliant with STIR/SHAKEN framework execution, and committed to preventing illegal robocalling and Voice Service Provider abuse
- **Policy Statement:** SRWS NETWORKS LLC maintains a zero-tolerance policy for illegal robocalls, spoofed caller IDs, and deceptive traffic practices

SRWS NETWORKS LLC's operations are governed by the FCC Registration Number, EIN, and RMD Filing ID listed above. All wholesale and commercial relationships are subject to the compliance obligations described in this RMP.

2. STIR/SHAKEN Implementation & Call Authentication

2.1 Framework Deployment

SRWS NETWORKS LLC has fully integrated STIR/SHAKEN digital certificates across its IP routing infrastructure. The company applies PASSporT signing to outbound SIP traffic and enforces attestation-level policy at all IP-to-PSTN handoff and interconnection points under its control.

- **Signing infrastructure:** SRWS operates or contracts a secure signing function (STI-C) that applies PASSporT tokens to outbound SIP INVITEs consistent with defined attestation rules.
- **Certificate management:** SRWS obtains service provider certificates from an authorized STI-CA and maintains documented processes for certificate request, issuance, renewal, and revocation.
- **SIP and signaling support:** The network supports SIP Identity header insertion and PASSporT transmission in accordance with ATIS/SIP Forum standards and industry best practices.

2.2 Attestation Standards

- Full Attestation (A): Assigned when the customer's identity is fully verified and they have authorized control over the specific originating calling number.
- Partial Attestation (B): Assigned when the origin of the call and customer identity are confirmed, but the specific caller ID number cannot be directly validated.
- Gateway Attestation (C): Applied to international or wholesale transit traffic entering the network where the originating identity cannot be independently validated.

Attestation assignment is enforced automatically at the point of call signing based on the outcome of the onboarding verification workflow described in Section 3. Exceptions require managerial approval and are logged for audit.

3. Know Your Customer (KYC) & Due Diligence Procedures

To comply with regulatory standards and mitigate illegal robocalling risks, SRWS NETWORKS LLC enforces strict Know Your Customer (KYC) onboarding for all commercial partners and wholesale voice clients:

- Business Verification: Mandatory collection of corporate registration documents, FCC Form 499 Filer ID/FRN details, tax identification (FEIN), and physical address verification.
- Traffic Scrutiny: Risk-based traffic evaluation prior to onboarding, distinguishing between standard commercial traffic and high-volume/automated call originations.
- Contractual Safeguards: Inclusion of strict anti-robocalling clauses in Service Agreements, prohibiting illegal caller ID spoofing and unauthorized automated dialing.
- Ongoing Review: Wholesale partner traffic profiles are periodically re-assessed against declared use cases; unexplained deviations trigger a compliance review.

4. Traffic Monitoring & Anomaly Detection

- Real-time Analytics: Automated monitoring systems analyze traffic patterns for robocall indicators (e.g., short-duration call bursts, high call volumes with low completion rates, or invalid/unassigned calling numbers).
- Telemetry Collection: Collection of SIP signaling logs, CDRs, and related call metadata to support detection and traceback.
- Traceback Cooperation: SRWS NETWORKS LLC fully cooperates with the Industry Traceback Group (ITG), the FCC, and law enforcement agencies. All traceback inquiries are investigated and responded to within required timelines.

5. Mitigation & Enforcement Actions

If suspicious or illegal call traffic is identified on the network, SRWS NETWORKS LLC applies a tiered enforcement process:

- Immediate Investigation: Suspect traffic patterns trigger an immediate internal compliance review.
- Service Suspension: SRWS NETWORKS LLC reserves the right to immediately block suspect call flows or suspend customer accounts violating anti-robocalling policies or federal guidelines.
- Termination: Repeated violations or failure to cooperate during traceback investigations result in immediate contract termination.
- Customer Notification: Written notification of suspected abuse and required remediation steps is provided except where prohibited by law or requested by law enforcement.

6. Recordkeeping and Reporting

- Record Retention: CDRs, signing/certificate records, KYC documentation, and mitigation records are retained for a minimum of two years, or longer where required by law or contract.
- Compliance Reporting: SRWS NETWORKS LLC will file and maintain accurate RMP certifications in the FCC's Robocall Mitigation Database and update filings as required.
- Internal Review: The RMP is reviewed periodically and updated in response to regulatory changes, audit findings, or incident learnings.

7. Certification and Signatory

I certify that the information contained in this Robocall Mitigation Plan is true and accurate, and that SRWS NETWORKS LLC has implemented the controls described herein.

Company: SRWS NETWORKS LLC

Federal EIN: 61-2278178

FCC Registration Number (FRN): 0038372579

RMD Filing ID: RMD0040045

Authorized Representative: Muhammad Junaid Malik

Title: CEO

Business Address: 1001 S. Main Street, Ste 600, Kalispell, MT 59901

Business Phone: 406-476-4030

Date of Issuance: August 25, 2026