



Robocall Mitigation Plan

Purpose:

This Robocall Mitigation Plan (RMP) describes the policies, technical controls, operational procedures, and enforcement measures implemented by APEX TELECO LLC to detect, prevent, and mitigate illegal robocalls in full compliance with 47 CFR § 64.6305. The RMP documents how APEX operates as an originating Voice Service Provider (VSP) and a domestic intermediate provider, and the measures the company employs when STIR/SHAKEN is applied with Attestations A and B.

1. Company Overview, Provider Role, and Operational Scope

- Company name: APEX TELECO LLC
- FCC Registration Number (FRN): 0037577814
- Principal office: 1001 S MAIN St . # 12393 KALISPELL, MT 59901
- Provider roles:
 - Originating Voice Service Provider (VSP)
 - Domestic Intermediate Provider
- Gateway status: APEX TELECO is a non-gateway provider and does not operate as a gateway for international ingress traffic.
- Geographic scope: APEX accepts and originates only domestic traffic. The company does not accept international-originating PSTN traffic.
- Traffic sources:
 - Direct retail customers (enterprises, call centers, and individual subscribers).
 - Vetted domestic wholesale partners and resellers.

- Network boundary and PSTN interconnects: APEX controls the IP-to-PSTN interconnection points used to originate calls onto the Public Switched Telephone Network (PSTN) and maintains policy enforcement at those egress points.

2. STIR/SHAKEN Implementation & Attestation Governance

APEX TELECO has implemented STIR/SHAKEN across its IP voice network consistent with industry standards and the company's security policy. The deployment includes PASSporT signing, certificate lifecycle management, attestation policy enforcement, and operational monitoring.

2.1 Overall STIR/SHAKEN Deployment

- Signing infrastructure:
 - APEX operates a secure signing function (STI-C / SHAKEN signing server) that applies PASSporT tokens to outbound SIP INVITEs per defined attestation rules.
 - Private keys for signing are stored in Hardware Security Modules (HSMs) or equivalent FIPS-compliant key stores. Access to signing keys is strictly limited and logged.
- Certificate management:
 - APEX obtains service provider certificates from an authorized STI-CA. Processes for certificate request, issuance, renewal, and revocation are documented and enforced.
 - Certificates and key usage are subject to documented change control and periodic audit.
- SIP and signaling support:
 - The network supports SIP identity header insertion and PASSporT transmission in accordance with RFCs and industry best practices.
 - Legacy or TDM interconnects are identified; signaling translation points apply policy checks and, where possible, signing or attestation mapping consistent with the RMP.

2.2 Attestation Policy and Governance

APEX enforces a clear attestation policy reflecting the company's verification capabilities and contractual relationships.

- Attestation A (Full):
 - Application: Attestation A is applied when APEX has verified the customer's legal identity and verified the customer's right to use the calling number (ANI).
 - Verification requirements:
 - Retail customers: Government-issued photo ID (or corporate equivalent), proof of telephone number ownership or LOA, billing and contact information, and signed service agreement acknowledging compliance with the RMP.
 - Direct numbering assignments: Documentation confirming the number assignment (e.g., LERG/NPAC records or assignment documents).
 - LOA: Signed Letters of Authorization when a customer uses numbers not directly assigned to them, including the number(s), authorized calling scope, and a dated signature.
 - Use cases: Typical retail subscribers, enterprise customers with direct number control, and cases where APEX can validate number ownership/control.
- Attestation B (Partial):
 - Application: Attestation B is applied to calls originating from vetted wholesale partners, resellers, or situations where APEX has a business relationship and KYC has been completed but APEX cannot directly validate the calling party's control of the ANI.
 - Verification requirements:
 - Wholesale partner due diligence: Business formation documents, tax ID/EIN, regulatory registrations, primary contacts, and documented calling use-case descriptions.

- Contractual requirements: Written agreements requiring partners to perform their own KYC, retain LOAs, and to promptly provide requested records for traceback.
 - Ongoing monitoring: Periodic reviews of partners' traffic to ensure consistency with declared profiles; failure to comply can result in suspension or downgrading of attestation allowance.
- Attestation C (Gateway): Not used. APEX does not operate as a gateway provider and therefore will not assert Attestation C.
- Attestation decision workflow:
 - A documented workflow maps onboarding verification results to attestation assignment (A or B).
 - Automated signing rules enforce attestation selection at the point of call origination.
 - Exceptions (temporary or transitional) require managerial approval and are logged for audit.

3. Robocall Mitigation Controls and Operations

APEX applies multiple layers of mitigation — preventive, detective, and corrective — to all traffic. These controls operate on retail accounts, wholesale partners, and at network interconnects.

3.1 Customer Onboarding, KYC and LOA Procedures

- Retail customers:
 - Identification: Collection of government-issued ID (for individuals) or corporate formation documents (for businesses), proof of physical address, billing information, and primary contacts.
 - Number control verification: Proof of number ownership, assignment records, or signed LOAs when claiming use of specific numbers.

- Service agreement: Execution of customer-facing terms and conditions that explicitly prohibit illegal robocalling and require cooperation with traceback requests.
- Wholesale partners and resellers:
 - Enhanced Due Diligence (EDD): Collection and verification of business registration, tax ID/EIN, key contacts, background checks for high-risk entities, and written escalation contacts for abuse and law enforcement requests.
 - LOA and records obligation: Partner contracts require maintenance of LOAs and detailed provisioning records and mandate immediate cooperation with traceback requests.
 - Pre-provisioning risk assessment: Expected traffic profile (CPS, geography, call types) documented; provisioning may be withheld if risk is unacceptable.
- LOA standards:
 - LOAs must specify the number(s), authorized use, effective date, and contain a wet or e-signature with name and contact information.
 - LOAs are retained for a minimum retention period (see section 4.4 Record Retention).

3.2 Contractual Controls and Acceptable Use Policy (AUP)

- AUP: All service agreements include a robust Acceptable Use Policy that bans unlawful robocalling, spoofing, and misuse of third-party numbers.
- Remedies: Agreements reserve the right to suspend or terminate service, apply rate-limits, or take other mitigations for violations.
- Audit and inspection rights: APEX reserves the right to request documentation and perform audits of partners to validate compliance.

3.3 Real-Time Monitoring, Analytics and Detection

- Monitoring platform:

- Continuous monitoring of per-account and per-trunk metrics such as Calls Per Second (CPS), Concurrent Calls (CC), Answer Seizure Ratio (ASR), Average Call Duration (ACD), and short-call rates.
- Collection of SIP signaling logs, CDRs, RTP metadata, and other relevant telemetry for analysis and traceback support.
- Detection mechanisms:
 - Threshold-based detection: Configurable thresholds per account/trunk trigger automated mitigations (e.g., CPS limits).
 - Behavioral and statistical analysis: Machine-learning models and statistical profiling identify deviations from expected call patterns (repeated short calls, sequential dialing, high disconnect rate).
 - Reputation feeds: Integration with third-party blocklists, reputation services, and industry feeds to flag suspicious destinations/origins.
- Alerting and escalation:
 - Alerts are classified by severity. High-severity alerts automatically create incident tickets and notify the Network Operations Center (NOC) and the Security/Compliance Officer.
 - Triage SLAs: Initial investigation begins within 2 hours of high-severity alert; lower severity within 24 hours.

3.4 Prevention and Automated Mitigations

- No-Signature, No-Route policy:
 - Outbound PSTN egress requires valid STIR/SHAKEN PASSporT signatures with appropriate attestation (A or B). Calls without required signatures are blocked at the egress edge except in documented transitional or lawful exceptions.
- Progressive mitigation controls:
 - Soft mitigation: Rate-limiting, interstitial warnings to the customer, temporary throttles.
 - Hard mitigation: Trunk suspension, route blocking, or full service termination for confirmed illegal activity.

- Challenge mechanisms:
 - For SIP-originated flows where feasible, utilize challenge/response techniques (e.g., interactive challenges, CAPTCHA-like flows) to verify human callers or reduce automated abuse.
- Flow control and per-customer limits:
 - Baseline call profiles set per-customer at onboarding. Deviations beyond defined multipliers trigger automated mitigations.

3.5 Traceback, Incident Response, and Law Enforcement Cooperation

- Traceback readiness:
 - Maintain sufficient logs (CDRs, SIP traces, signaling and routing metadata) to support industry and law enforcement traceback processes.
 - Maintain an internal traceback runbook aligned to ITG processes and industry best practices.
- Incident response process:
 - Detection → Triage → Containment → Remediation → Post-incident review.
 - Containment options: Rate-limits, route blocking, account suspension, or number-level blocks.
- Law enforcement and ITG cooperation:
 - APEX will respond to traceback and lawful requests from the FCC, Industry Traceback Group (ITG), and law enforcement promptly.
 - Initial acknowledgement within 24 hours for documented requests; APEX aims to provide substantive data and assistance per the request timeline.
- Notification procedures:
 - When a customer is suspected of illegal activity, APEX will notify the customer of mitigation actions and request corrective steps where appropriate, except where prohibited by law or requested by law enforcement.

4. Enforcement, Escalation, Auditing and Recordkeeping

4.1 Enforcement and Escalation

- Enforcement tiers:
 - Tier 1 — Automated mitigations and notifications (rate-limits, warns).
 - Tier 2 — Manual investigation, temporary suspension pending remediation.
 - Tier 3 — Permanent route blocking and service termination for confirmed illegal robocalling or failure to remediate.
- Customer communication:
 - Written notification of suspected abuse, actions taken, and remediation steps required. Emergency mitigations may be applied without prior notice when needed to protect the network or public interest.
- Appeals and remediation:
 - Customers may appeal mitigation actions by providing corroborating evidence (corrected LOA, revised configuration, etc.). Appeals are reviewed by Security/Compliance Officer and NOC.

4.2 Audits and Reviews

- Internal audits:
 - Regular internal reviews of RMP effectiveness, STIR/SHAKEN operations, and KYC processes. Frequency: quarterly operational reviews and annual comprehensive RMP review.
- External audits:
 - Third-party audits or assessments may be performed as required by law, industry best practices, or contractual obligations.
- Continuous improvement:
 - Findings from incidents, audits, and regulatory updates drive RMP updates and improvements through a formal change-control process.

4.3 Record Retention

- Retention policy:
 - Maintain CDRs, SIP logs, LOAs, KYC documents, incident tickets, and mitigation records for a minimum of two years (or longer when required by law or contractual obligations).
 - Ensure secure storage with access controls and auditing.
- Data access and disclosure:
 - Provide requested records to law enforcement and regulatory bodies consistent with legal processes and timelines.

4.4 Metrics and Reporting

- Operational metrics:
 - Track and report on key metrics such as number of mitigations, time-to-detect, time-to-mitigate, number of traceback responses, and volume of traffic with Attestation A vs. Attestation B.
- Compliance reporting:
 - Provide required RMP attestations and updates to the FCC or other regulatory bodies as required.

5. Governance, Roles, and Training

- Roles and responsibilities:
 - Authorized Representative / CEO: Ultimate responsibility for ensuring RMP compliance and signing authority.
 - Security & Compliance Officer: RMP ownership, KYC governance, liaison with legal and law enforcement.
 - Network Operations Center (NOC): Real-time monitoring, initial investigations, and operational mitigations.
 - Customer Success / Account Management: Onboarding, LOA collection, customer communications, and remediation coordination.

- Legal Counsel: Review of contractual language, regulatory changes, and law enforcement requests.
- Training:
 - Regular staff training on robocall regulations, RMP procedures, STIR/SHAKEN operations, and incident response.
 - Periodic tabletop exercises simulating traceback and mitigation scenarios.

6. Technical Appendices (summary descriptions)

- Signing and Certificate Management Appendix:
 - Description of HSM usage, key access controls, certificate lifecycle steps, and revocation procedures.
- Monitoring and Detection Appendix:
 - Overview of telemetry collection, thresholds, ML models, and third-party integrations.
- Onboarding and LOA Templates:
 - Standard LOA template format and required fields.
- Traceback Runbook:
 - Step-by-step procedures for responding to ITG/FCC/law enforcement traceback requests, including data elements provided and typical SLAs.

7. Certification and Signatory

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

Company: APEX TELECO LLC

FCC Registration Number (FRN): 0037577814

Authorized Representative: Rabiya Shahid

Title: CEO

Business Address: 1001 S . MAIN St . # 12393 KALISPELL MT 59901

Date of Issuance: April 6th 2026