Robocall Mitigation Plan

GoldAndSilver, LLC | Updated draft for review | November 17, 2026

UPDATED DRAFT - COMPLETE THE REMAINING DETAILS
GoldAndSilver has confirmed that it operates a switch, uses its own STIR/SHAKEN certificate, monitors traffic, verifies customers and upstream providers, and responds to tracebacks within 24 hours. Complete the remaining bracketed details before filing.

1. Company information and scope

Legal name: GoldAndSilver, LLC
Address: 390 Northeast 191st Street 45951, Miami, FL 33179
CEO: Eric Shires
Telephone: 208-480-1750 **Email:** eric.shires@goldsilvertech.online
EIN: 41-4344990

Business: U.S. wholesale VoIP termination and origination. **Call-chain roles:** [Describe the actual call flows and confirm whether the company acts as a gateway or non-gateway intermediate provider.]

Robocall mitigation contact: Eric Shires, CEO; eric.shires@goldsilvertech.online; 208-480-1750. The company confirms its 24-hour traceback response capability.

2. Program purpose and oversight

The following controls are intended to prevent the origination, carrying or processing of illegal robocalls and caller ID spoofing, as applicable to each role. The designated compliance officer will oversee implementation, document investigations and corrective actions, and review the program at least annually and when business practices or applicable requirements change. [Identify responsible person and actual review schedule.]

3. Customer onboarding and renewal

- Before activation, collect and verify legal business name, business address, authorized contacts, ownership or control information, and intended use of service. Confirm the customer's identity using reliable, independent records and investigate material inconsistencies.
- Review expected call sources, destinations, volume, call types, numbering and authorization to use caller IDs. Obtain information on consent, calling practices, opt-out processes and scripts or recordings where relevant. Decline service where material questions cannot be resolved.
- Require written contract terms prohibiting illegal robocalls, spoofing and other unlawful traffic; require customers and resellers to cooperate with investigations and tracebacks. Reverify customer information and traffic patterns upon renewal and when material changes or risk indicators arise.

4. Know your upstream providers

For each upstream provider, identify the legal entity, business and operational contacts, locations, services, traffic sources and expected calling patterns. Check applicable FCC registration and Robocall Mitigation Database entries and resolve missing or inconsistent information before accepting traffic. Reassess the relationship periodically and after complaints, traceback requests, ownership changes or unusual traffic. Record review results and escalation decisions. [Identify actual checks, sources, review frequency and responsible staff.]

5. Traffic monitoring and call analytics

Review call detail records and relevant network alerts for unusual call volumes or bursts, repeated short-duration calls, rapid changes in caller ID, invalid or unauthorized numbers, abnormal completion patterns, complaints and other indicators of potentially illegal calling. Compare traffic with the customer's declared use; investigate alerts in context. No single metric alone proves a call is illegal.

Actual analytics: [Identify every system and third-party vendor used, or state accurately that no analytics system is used. Describe the data reviewed, alert thresholds, review frequency, human review and responsible personnel. Identify which functions are performed by upstream or downstream providers.]

6. Investigation, blocking and corrective action

Log complaints, traceback requests and internal alerts. Preserve relevant call records and identify the customer or upstream source. Request supporting information and assess the explanation against call data and applicable rules. Where warranted, restrict or block affected traffic, suspend service, require corrective action, or terminate the relationship. Document the basis for action and maintain an escalation and appeal process for possible false positives. Comply with applicable blocking and notification rules.

7. Traceback and incident response

The company must be prepared to respond fully to traceback requests from the FCC, law enforcement and the registered industry traceback consortium within 24 hours, as applicable. The company confirms this commitment and 24-hour availability. The responsible team should record receipt time, preserve relevant records, identify the immediate upstream source and downstream recipient, promptly provide responsive information and escalate unresolved cases. Document follow-up and remediation.

8. STIR/SHAKEN implementation or exemption

Implementation status: GoldAndSilver confirms that it operates its own VoIP switch and uses its own STIR/SHAKEN certificate. [Specify full or partial implementation, the SPC token status, and signing and verification arrangements for each relevant role and network segment.]

Any exemption or extension: [Identify the applicable FCC rule or order, affected services and network segments, and detailed facts supporting eligibility. Do not claim an exemption until verified.] The FCC has recognized an exemption for providers that lack control over the infrastructure needed to implement STIR/SHAKEN: First Caller ID Authentication Report and Order, FCC 20-42, paragraph 40. If relying on it, identify the provider controlling the relevant infrastructure, explain why GoldAndSilver cannot implement the framework, describe the applicable call flows and how these facts were verified. A small-provider classification by itself is not a current basis for the expired small-provider extensions. An implementation exemption does not eliminate applicable robocall mitigation obligations.

9. Records, training and review

Maintain customer and upstream due-diligence records, relevant call detail records, monitoring and investigation logs, complaints, traceback responses and corrective actions in accordance with applicable requirements and company retention policy. Limit access to authorized personnel and protect sensitive information. Train relevant employees on onboarding, traffic review, escalation and traceback procedures. [Specify retention periods, systems, training frequency and accountable staff.]

10. Approval and filing checklist

- Verify every statement describes controls actually implemented; replace all bracketed fields and remove inapplicable procedures.
- Confirm network roles, current STIR/SHAKEN status and the facts supporting any exemption or extension. Review all other RMD certification questions, including applicable enforcement history, independently.
- Confirm the designated mitigation contact and 24-hour traceback process, then have an authorized officer review and approve the plan before submission. Keep the filing current under applicable FCC requirements.

Authorized officer: Eric Shires, CEO **Approval date:** _____

Reference materials

FCC guidance on RMD plan requirements: https://docs.fcc.gov/public/attachments/DA-26-872A1.pdf
FCC guidance on STIR/SHAKEN status and exemptions: https://docs.fcc.gov/public/attachments/DA-26-72A1.pdf
FCC discussion of the lack-of-infrastructure exemption: https://docs.fcc.gov/public/attachments/FCC-24-120A1.pdf