



PO Box 255
Conyers GA 30012
info@selectivesolutions.com
www.selectivesolutions.com

| Networks | Computers | Cyber Security | Compliance | Data Security | Phone Systems |

Robocall Mitigation Plan

Filed by Selective Solutions
FRN: 0031445448

1. Company Information

Legal Entity: Selective Solutions, LLC.
Doing Business As: Selective Solutions LLC
Address: 1479 Highway 212 SW, Conyers, GA 30094

Primary Contact:

Name: Kenneth Holmes
Title: CEO
Phone: 770-929-1155 x 111
Email: ken@selectivesolutions.com

2. STIR/SHAKEN Implementation Status

We do not directly implement STIR/SHAKEN authentication because we do not operate originating or terminating switching infrastructure capable of applying STIR/SHAKEN signatures at the network switch level.

1. We use Skytel OCN 622J as our upstream SIP vendor. Skytel OCN 622J provides SIP trunking, number provisioning, routing and applicable network-level STIR/SHAKEN functionality.
2. All DID's used by our customers are provisioned through Skytel OCN 622J.
3. Inbound calls are routed by Skytel OCN 622J to the applicable customer PBX system supported by Selective Solutions LLC.
4. Outbound calls from customer PBX systems are routed to Skytel OCN 622J for origination into the PSTN.
5. STIR/SHAKEN authentication and attestation are applied at the network level by Skytel OCN 622J before outbound calls enter the PSTN.
6. We do not alter, strip, or obscure STIR/SHAKEN identity headers or attestation information passed through our systems.
7. We coordinate with Skytel to address traceback requests, suspicious traffic notices, call routing issues, number provisioning issues, and STIR/SHAKEN-related concerns.
8. We only provision service to business customers with verified identities.

3. Robocall Mitigation Practices

We employ the following measures to prevent and mitigate unlawful robocalls:

Know Your Customer (KYC):

We do not use a third-party provider for Know Your Customer (KYC). Instead, we implement an internal customer verification process for new and existing customers that includes:

1. Collection and verification of customer identity information, including legal business name, physical address, billing contact, technical contact and other relevant contact information.
2. Verification of business registration or business existence through publicly available records,

where applicable, such as Secretary of State filings, business websites, or other publicly available business records.

3. Collection of Employer Identification Number (EIN) or Tax ID where applicable
4. Review of the nature of the customer's business and intended use of our services before provisioning services.
5. Screening for high-risk industries or use cases associated with illegal robocalling or other unlawful calling activity.
6. Application of KYC procedures to existing customers through ongoing billing relationships, support interactions, PBX management, service-change requests, number additions, and review of customer activity that appears inconsistent with their stated use case.
7. Additional review when an existing customer requests unusual service changes, such as increased outbound calling capability inconsistent with the customer's known use case.
8. Maintenance of customer records and documentation for audit, compliance, support, and traceback requests.
9. Ongoing monitoring for suspicious or anomalous traffic patterns
10. Immediate investigation and mitigation, including suspension, if suspicious robocall activity is detected.

Analytics and Monitoring:

We do not currently use a separate third-party vendor for robocall analytics. Instead, we rely on internal monitoring, direct customer relationships, available call information, customer support activity and notices or alerts from Skytel, the FCC, law enforcement, the Industry Traceback Group, customers, or other relevant parties.

Our analytics and monitoring practices include:

1. Monitoring for suspicious increases in traffic volume, complaints, traceback requests, SIP vendor notices, and other indicators of potentially unlawful calling activity.
2. Reviewing available call information if suspicious activity is identified.
3. Coordinating with Skytel regarding suspicious traffic, traceback requests, call routing issues, number provisioning issues, and STIR/SHAKEN-related concerns.
4. Requiring customer explanation, corrective action, or additional documentation where appropriate.
5. Mitigation actions may include traffic restriction, suspension or termination of service.

Know Your Upstream Provider (KYUP):

We use Skytel OCN 622J as our singular upstream SIP vendor for SIP trunking, number provisioning, routing and applicable network-level STIR/SHAKEN functionality. We maintain a direct business relationship with Skytel OCN 622J and coordinate with Skytel OCN 622J regarding suspected illegal traffic, traceback requests, call routing issues, number provisioning issues, and STIR/SHAKEN-related concerns.

We do not accept third-party traffic for transit. Outbound calls originate only from our business customers using PBX systems we support, and inbound calls are received from Skytel for delivery to those customers.

4. Prior Law Enforcement, Regulatory Agency, or Commission Action

We disclose that we were named in an FCC action concerning our Robocall Mitigation Database certification and robocall mitigation plan.

The matter involved the FCC's Wireline Competition Bureau and Enforcement Bureau. It began under File No. EB-TCD-24-00036891 after the FCC identified companies whose RMD certifications and robocall

mitigation plans had not been updated with information required by the February 26, 2024 deadline. The matter was later assigned File No. EB-TCD-25-00038590.

The Wireline Competition Bureau notified affected companies on March 29, 2024 and required updates by April 29, 2024. On December 10, 2024, the Enforcement Bureau issued a Show Cause Order directing affected companies to either cure the deficiencies or explain why their certifications should not be removed from the RMD.

On August 25, 2025, the Enforcement Bureau issued DA 25-737, which included our company in Appendix A. The Order stated that the listed companies' certifications were deficient because the robocall mitigation plans were either missing or did not include required information, and the certifications also lacked required information.

The findings were limited to deficiencies in our RMD certification and robocall mitigation plan. The Order did not identify a company-specific finding that we originated illegal robocalls, knowingly facilitated illegal robocalling, engaged in illegal spoofing, or transmitted unlawful traffic.

The final determination was the August 25, 2025 Order removing our certification from the Robocall Mitigation Database until refiling approval was obtained from the Wireline Competition Bureau and Enforcement Bureau.

We have since updated our RMD filing and understand that we have been provisionally reinstated in the Robocall Mitigation Database, subject to further FCC review and any additional revisions requested by the Bureau.

5. Traceback Commitment and Plan Governance

We remain committed to responding fully and within 24 hours to call traceback requests from the Commission, law enforcement, and the traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers.

We review and maintain our robocall mitigation program on an ongoing basis. We will update our filing within 10 business days when filing information change or when there are material changes to our services, traffic profile, upstream provider relationships, customer vetting procedures, monitoring practices, or robocall mitigation controls.

Signed:



CEO

Selective Solutions, Inc.

Date: July 2, 2026