



Solid Rock Solutions Computer Consulting

STIR/SHAKEN Alignment & Robocall Mitigation Plan

1. Purpose & Scope

This plan outlines how Solid Rock Solution Computer Consulting (“SRSCCTEK”) aligns with **STIR/SHAKEN** requirements and implements **robocall mitigation practices** to prevent unlawful caller ID spoofing, spam, and fraudulent outbound calls.

The plan applies to:

- All outbound voice traffic
 - All business phone numbers owned, leased, or assigned to Solid Rock Solutions Computer Consulting
 - Any third-party VoIP, SIP, or telecom providers used by Solid Rock Solutions Computer Consulting
-

2. Company Profile

- **Business Type:** IT & Computer Consulting Services
 - **Call Type:** Primarily low-volume, human-initiated business calls
 - **Use Case:** Client support, project coordination, sales inquiries
 - **Automated Calling:** None (no autodialers, robocall campaigns, or bulk voice marketing)
-

3. STIR/SHAKEN Compliance Strategy

3.1 Calling Number Authentication

- Solid Rock Solutions Computer Consulting uses **verified business phone numbers** registered to the company.
- Outbound calls are placed through **STIR/SHAKEN-enabled VoIP providers** capable of:

- Signing calls with **A-level or B-level attestation** where applicable
- Passing identity headers intact across the call path

3.2 Attestation Levels

- **A Attestation:** Used when Solid Rock originates calls from numbers it owns and controls.
- **B Attestation:** Used when number ownership exists but call origination is partially managed by a provider.
- **C Attestation:** Avoided whenever possible.

Solid Rock works with providers to maintain the **highest possible attestation level**.

4. Robocall Mitigation Measures

4.1 Prohibited Activities

Solid Rock **does not**:

- Place robocalls or prerecorded messages
- Use autodialers or predictive dialers
- Engage in unsolicited telemarketing
- Spoof caller ID numbers

4.2 Allowed Call Practices

- Calls are **human-initiated**
 - Calls are made for legitimate business purposes only
 - Calling hours comply with TCPA guidelines
 - Caller ID accurately reflects Solid Rock's business identity
-

5. Traffic Monitoring & Abuse Prevention

5.1 Call Volume Controls

- Low, consistent call volumes aligned with consulting operations
- No sudden spikes or burst calling patterns

5.2 Monitoring & Alerts

- Solid Rock relies on its telecom provider's:

- Spam analytics
- Call reputation monitoring
- Automated blocking of suspicious activity

5.3 Complaint Handling

- Any spam or spoofing complaints are:
 - Logged internally
 - Investigated promptly
 - Escalated to the telecom provider if necessary
-

6. Third-Party Provider Management

Solid Rock only uses providers that:

- Support STIR/SHAKEN signing and verification
- Maintain FCC-compliant robocall mitigation programs
- Provide call traceability and reporting

Providers are reviewed periodically for continued compliance.

7. Recordkeeping & Documentation

Solid Rock maintains:

- Proof of number ownership
 - Provider contracts and compliance statements
 - Call logs (as provided by carriers)
 - Records of any complaints and resolutions
-

8. FCC Robocall Mitigation Database

- Solid Rock certifies that it does not originate illegal robocalls.
 - This mitigation plan is maintained and updated as needed.
 - Documentation is available upon request by carriers or regulators.
-

9. Review & Updates

This plan is:

- Reviewed annually
 - Updated when regulations change
 - Updated when telecom providers or call practices change
-

10. Contact Information

Compliance Contact:

Solid Rock Solution Computer Consulting

 angelov@srsccetek.com

 570-290-7717 x1