

A. Filer Identification

- Legal Business Name: Rader Solutions, LTD
 - Other DBA Names: RaTel, RADER
 - Parent Company: Courser
 - FRN: 0024664732
 - Business Address: 838 Coolidge Dr, Lafayette LA 70503
 - Primary Robocall Mitigation Contact:
 - Name/Title: Tyler Robertson, COO
 - Email: ratel@radersolutions.com
 - Phone: 337-205-4652
-

B. Description of Role in Call Path

RADER provides managed PBX and unified communications services for business customers using three upstream providers:

1. Reinvent Telecom
 - Reinvent provides the hosted PBX platform, SBC infrastructure, SIP trunks, numbering resources (DIDs), and outbound PSTN origination.
 - Reinvent signs or authenticates calls (via STIR/SHAKEN) according to their FCC obligations.
2. Microsoft Teams / Microsoft Calling Plans
 - Microsoft provides direct PSTN connectivity via Teams Calling Plans and/or Operator Connect.
 - Microsoft's network, not the MSP, performs any call authentication or STIR/SHAKEN obligations.
3. Bandwidth.com
 - RADER is currently migrating customers away from its legacy PBX Asterisk Systems which relied on Bandwidth.com SIP Trunks for PSTN connectivity and will be completely moved to Reinvent Telecom by 2027.
 - RADER does not manage the SBCs and relies on Bandwidth.com to sign or authenticate calls (via STIR/SHAKEN) according to their FCC obligations and applies best practices to make sure all traffic relayed is correct and verified for use by the customer.

The MSP does *not* operate SBCs, SIP gateways, or any PSTN interconnection points; therefore the MSP does not originate PSTN calls and does not control SIP signaling. The MSP instead manages customer configurations, user licensing, dial plans, and PBX feature administration.

C. STIR/SHAKEN Status

Because the MSP does not control any SBCs and does not originate PSTN calls:

- All STIR/SHAKEN authentication is performed exclusively by Reinvent Telecom, Microsoft and Bandwidth.com.

- The MSP performs no call signing, does not possess SPC tokens, and does not maintain certificates.

This means the MSP falls under the category of a non-originating reseller whose responsibilities relate to customer vetting, configuration integrity, and supporting upstream carrier compliance—not direct authentication.

D. Robocall Mitigation Program

1. Customer Vetting (KYC)

- Every customer must have an existing MSP support contract.
- Voice services are only added after manual business verification, including:
 - Corporate identity verification,
 - Valid business address and contact details,
 - Review of intended voice use cases.
- Customers with prohibited use cases (high-risk outbound dialing, lead-gen robocalling, etc.) are not accepted.

2. Number Assignment & Caller ID Integrity

- All DIDs, numbers, and SIP trunks are purchased from Reinvent Telecom, Microsoft or Bandwidth.com.
- Caller ID (CLI/CNAM) is controlled exclusively by these carriers through their portals.
- Customers cannot override or spoof caller ID because the MSP's platforms enforce locked caller ID settings within Teams, Reinvent PBX, and Rader's Asterisk portals.
- All outbound calls present only:
 - Reinvent-assigned DIDs, or
 - Microsoft-assigned DIDs (Teams Calling Plan numbers).
 - Bandwidth.com-assigned DIDs that are whitelisted by individual IP per company that matches their available outbound caller IDs.

3. No Customer Control of Signaling / SBC

- Customers have no access to SBCs or SIP manipulation layers.
- MSP also has no ability to modify SIP headers, caller ID, attestation, or routing.
- Reinvent and Microsoft fully control signaling, STIR/SHAKEN handling, and routing.
- Rader's Asterisk Platform uses a set list of Caller IDs that are allowed per customer, and blocks all traffic that does not include a Caller ID or incorrect Caller ID. There is no additional information passed besides Caller ID, and originating IP so no SIP Header adjustments or additional changes can be made.

4. Monitoring & Abuse Detection

Even without SBC control, the MSP provides monitoring through:

- Reinvent Telecom analytics dashboards (call volume, durations, failure patterns).
- Microsoft Teams admin center call analytics and quality dashboards.

- Rader's Asterisk Platform includes outbound call monitor reports and other analytics which trigger tickets in their MSP Ticketing System (call volume, durations, failure patterns.)
- Internal alerting for:
 - Sudden spikes in call volume,
 - Abnormal short-duration call patterns,
 - Rapid sequential dialing,
 - Excessive international attempts (if enabled for the tenant).
 - SIP Failures and reason

Suspicious activity leads to immediate investigation and possible suspension of the customer's outbound calling until reviewed.

5. Traceback Commitment (24-Hour Compliance)

Even though the MSP does not originate PSTN traffic, the MSP commits to:

- Respond to all traceback requests within 24 hours,
 - Provide customer account information, call logs, and configuration data to:
 - The FCC,
 - Law enforcement,
 - The Industry Traceback Group (ITG),
 - Reinvent Telecom, Bandwidth.com or Microsoft's compliance teams.
-

6. Enforcement and Remediation

- If suspicious or illegal usage is identified:
 1. Immediate outbound calling suspension,
 2. Incident review and customer contact,
 3. Possible permanent service removal if misuse is confirmed.
 - Reinvent, Bandwidth.com and Microsoft may impose their own blocks at the carrier level, and the MSP will coordinate accordingly.
-

7. Upstream Provider Verification

- The MSP verifies quarterly that both Reinvent Telecom, Bandwidth.com and Microsoft remain properly listed in the FCC Robocall Mitigation Database.
 - MSP ensures all customer PSTN traffic flows only through providers active in the RMD.
-

8. Governance & Plan Updates

- A designated compliance manager oversees all mitigation activities.
 - The plan is reviewed annually or upon any material operational change.
 - RMD filings and CORES data are updated promptly to comply with new FCC accuracy/timeliness requirements.
-

E. Officer Attestation

“I certify under penalty of perjury that this robocall mitigation plan is accurate, that RADER does not originate PSTN traffic and relies on upstream carriers for STIR/SHAKEN, and that RADER will respond to all traceback requests within 24 hours.”