

Robocall Mitigation Plan

AffinityUnified (Affinity Tech Solutions)

Filing Type: Voice Service Provider Without a STIR/SHAKEN
Implementation Obligation

Date: **3/24/2026** • Plan Version: 1.0

1. Provider Identification

Business Name: AffinityUnified (a subsidiary of Affinity Tech Solutions)

Business Address: **2801 S Bay St, Suite 137, Eustis, FL 32726**

FCC Registration Number (FRN): 0033191545

OCN: N/A — AffinityUnified does not hold an Operating Company Number, as it does not directly hold numbering resources.

Contact for Robocall Mitigation Issues:

- **Name:** Jeremy Valverde
- **Title:** Owner / Principal
- **Email:** jeremy@affinitytechsolutions.com
- **Phone:** 407-385-1611 x199

Principals, Affiliates, Subsidiaries, and Parent Companies: Affinity Tech Solutions, LLC

Prior Enforcement Actions: Neither AffinityUnified nor any affiliated entity has been subject to any Federal Communications Commission or other law enforcement agency action or investigation in the prior two years due to suspected involvement with illegal robocalling or spoofing, or due to a deficiency in its Robocall Mitigation Database certification.

2. Role in the Call Chain

AffinityUnified operates as a **voice service provider directly serving end users**. AffinityUnified provides hosted UCaaS/VoIP services to small and medium business customers under its own brand through a white-label reseller arrangement with SkySwitch (a BCM One company), which owns and operates the underlying network infrastructure, including all SIP trunking, call routing, and PSTN interconnection.

AffinityUnified does not operate as a gateway provider or intermediate provider.

3. STIR/SHAKEN Implementation Status and Exemption Basis

Implementation Status: AffinityUnified has not implemented the STIR/SHAKEN authentication framework on any portion of its network.

Basis for Exemption: AffinityUnified is exempt from the STIR/SHAKEN implementation obligation because it lacks control over the network infrastructure necessary to implement STIR/SHAKEN, pursuant to 47 CFR § 64.6305(d)(2)(i). Specifically:

- AffinityUnified does not own or operate switching equipment, SIP infrastructure, or PSTN interconnection facilities.
- All voice traffic originated by AffinityUnified's end-user customers traverses the SkySwitch platform, which is owned and operated by SkySwitch/BCM One.
- SkySwitch maintains its own STIR/SHAKEN implementation, including its own SPC token and digital certificate, and performs caller ID authentication (call signing) for outbound calls originated on its platform.
- AffinityUnified does not have the technical capability to independently authenticate, sign, or assign attestation levels to calls, as it has no direct access to the signaling or media path of calls at the network level.

AffinityUnified relies on SkySwitch's STIR/SHAKEN implementation for caller ID authentication of all calls originated by its customers. Despite this exemption, AffinityUnified has implemented the robocall mitigation program described below to take affirmative, reasonable steps to prevent the origination of illegal robocall traffic.

4. Robocall Mitigation Program

4.1 Know Your Customer (KYC) — Affirmative Measures to Prevent Illegal Robocalls

AffinityUnified has implemented the following customer vetting and onboarding procedures designed to prevent new and renewing customers from using its services to originate illegal robocalls:

Pre-Activation Vetting:

- All prospective customers must provide valid business identification, including legal business name, physical address, and tax identification number (EIN) or equivalent, prior to service activation.
- AffinityUnified verifies the identity and legitimacy of each prospective customer by confirming business registration through publicly available records (e.g., state secretary of state databases, business directories).
- Prospective customers must identify the primary use case for their voice services (e.g., general business communications, customer support). Applicants whose stated use case suggests high-volume outbound calling, telemarketing, or lead generation are subject to enhanced review.
- AffinityUnified does not knowingly provision service to entities engaged in illegal robocalling, caller ID spoofing for fraudulent purposes, or any activity that would violate the Telephone Consumer Protection Act (TCPA) or the Truth in Caller ID Act.

Acceptable Use Policy (AUP):

- All customers must acknowledge and agree to AffinityUnified's Acceptable Use Policy as a condition of service, which explicitly prohibits:
 - Origination of illegal robocalls or autodialed calls in violation of the TCPA.
 - Caller ID spoofing with the intent to defraud, cause harm, or wrongfully obtain anything of value.
 - Use of AffinityUnified services for any purpose that violates federal, state, or local law.
- The AUP reserves AffinityUnified's right to immediately suspend or terminate service for any customer found to be originating illegal robocall traffic or engaging in prohibited activity.

Ongoing Monitoring and Re-Verification:

- AffinityUnified reviews customer accounts on a periodic basis and upon receipt of any complaint, traceback request, or suspicious activity alert.
- Customers with unusual call patterns, high call volumes relative to their stated use case, or calls flagged by SkySwitch's fraud monitoring systems are subject to

additional review, which may include direct outreach to the customer, temporary service suspension pending investigation, or permanent termination.

4.2 Call Analytics and Traffic Monitoring

AffinityUnified utilizes the following systems and procedures to identify and block illegal robocall traffic:

- **SkySwitch Platform Fraud Monitoring:** AffinityUnified relies on SkySwitch's built-in fraud detection and call monitoring capabilities, which are integrated into the SkySwitch platform. These tools provide real-time alerts for anomalous call patterns, including unusually high call volumes, rapid short-duration calls, and calls to known high-risk destinations. SkySwitch's fraud protection system is capable of automatically restricting or blocking suspicious traffic.
- **Manual Review and Escalation:** Upon receiving any alert from SkySwitch's fraud monitoring system, or upon identification of suspicious calling activity through AffinityUnified's own review of call detail records (CDRs) and customer usage reports, AffinityUnified investigates the activity and takes appropriate action, including customer contact, service suspension, or termination.
- **Third-Party Analytics Vendors:** At this time, AffinityUnified does not utilize any third-party call analytics vendors beyond the capabilities provided by SkySwitch. AffinityUnified will evaluate the adoption of additional analytics tools as its customer base and call volumes grow, or as the FCC's requirements evolve.

4.3 Upstream Provider Awareness

AffinityUnified's sole upstream voice service infrastructure provider is SkySwitch (operated by BCM One). AffinityUnified has confirmed that SkySwitch maintains an active and compliant filing in the FCC's Robocall Mitigation Database and has implemented STIR/SHAKEN on its platform. AffinityUnified does not accept or transit voice traffic from any other upstream provider.

4.4 Caller ID and Number Management

- AffinityUnified provisions telephone numbers to its customers exclusively through the SkySwitch platform. All numbers are sourced from SkySwitch's carrier relationships and are subject to SkySwitch's number management and porting policies.
- AffinityUnified does not permit customers to originate calls using caller ID numbers that they are not authorized to use.

Caller ID assignment is managed within the SkySwitch platform, and customers may only display numbers that have been properly provisioned to their account.

- If AffinityUnified becomes aware of any instance of unauthorized caller ID manipulation by a customer, it will immediately investigate and take corrective action, up to and including service termination.

5. Traceback Response Commitment

AffinityUnified commits to responding fully and within twenty-four (24) hours to all traceback requests received from:

- The Federal Communications Commission (FCC)
- Federal and state law enforcement agencies
- The Industry Traceback Group (ITG) or any consortium designated by the FCC to conduct traceback investigations

AffinityUnified will cooperate fully with such entities in investigating and, where necessary, terminating or blocking traffic identified as illegal robocall traffic. AffinityUnified will preserve relevant call detail records and customer information as needed to support traceback and enforcement efforts, consistent with applicable law.

Traceback Contact:

- **Name:** Jeremy Valverde
- **Title:** Owner / Principal
- **Email:** support@affinitytechsolutions.com
- **Phone:** 407-385-1611

6. Enforcement and Remediation Procedures

Upon identification of a customer originating illegal robocall traffic, whether through internal monitoring, SkySwitch alerts, traceback requests, or external complaints, AffinityUnified will take the following actions:

1. **Immediate Investigation:** AffinityUnified will promptly investigate the reported activity by reviewing available call detail records, customer account information, and any information provided by the reporting party.
2. **Interim Suspension:** Where the investigation indicates that illegal robocall traffic is being originated, AffinityUnified will immediately suspend the offending customer's outbound calling capability pending resolution.
3. **Customer Notification:** AffinityUnified will notify the customer of the suspension and the basis for it, and provide the customer an opportunity to respond.

4. **Termination:** If the investigation confirms that the customer originated illegal robocall traffic, or if the customer fails to provide a satisfactory explanation, AffinityUnified will permanently terminate the customer's service.
5. **Reporting:** AffinityUnified will report confirmed illegal robocall activity to SkySwitch and, where appropriate, to the FCC and law enforcement.

7. Plan Maintenance and Updates

AffinityUnified will review and update this Robocall Mitigation Plan at least annually, or more frequently as required by changes to FCC rules, changes to AffinityUnified's business operations or upstream provider relationships, or as informed by enforcement trends and best practices.

AffinityUnified will update its Robocall Mitigation Database filing within ten (10) business days of any material change to the information contained in its filing, as required by 47 CFR § 64.6305(d)(5).

Certification

I, Jeremy Valverde, as the authorized representative of AffinityUnified (Affinity Tech Solutions), certify that:

1. All calls originated by AffinityUnified on its network are subject to the robocall mitigation program described above.
2. AffinityUnified's prior certification has not been removed by Commission action, and AffinityUnified has not been prohibited from filing in the Robocall Mitigation Database.
3. AffinityUnified has not implemented the STIR/SHAKEN authentication framework on any portion of its network due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN.

Signature:

Printed Name: Jeremy Valverde

Title: Owner / Principal

Date: 3/24/2026