

Robocall Mitigation Program Description

Company Name: Scyber LLC

Date of Issuance: Feb 2026

Filing Type: Voice Service Provider without a STIR/SHAKEN obligation

1. Provider Classification and Exemption from STIR/SHAKEN Implementation

Scyber LLC ("Scyber") operates as a non-facilities-based white-label reseller of interconnected VoIP services. Scyber provides voice communications to end-users using North American Numbering Plan (NANP) resources.

Exemption Claimed: 47 CFR § 64.6304(b)

Detailed Explanation of Exemption: Scyber does not own, manage, or control the underlying physical network infrastructure, IP nodes, switching fabric, or session border controllers required to technically implement the STIR/SHAKEN authentication framework. Scyber does not possess its own Operating Company Number (OCN). Consequently, Scyber is structurally incapable of obtaining an SPC token from the STI-PA (Secure Telephone Identity Policy Administrator) and cannot independently generate the digital certificates required to cryptographically sign calls. Because of this lack of control over the necessary network infrastructure, Scyber is exempt from the direct implementation obligations of § 64.6301 and fulfills its regulatory duties by ensuring all originated traffic is authenticated by a compliant upstream provider.

2. Upstream Provider & Technical Authentication

Scyber relies exclusively on its upstream platform provider, **SkySwitch (BCM One)**, to provide the underlying voice network infrastructure.

- All calls originated by Scyber's end-users traverse the SkySwitch network.
- SkySwitch, acting as the facilities-based carrier, holds the necessary tokens and certificates to perform full STIR/SHAKEN cryptographic signing (Attestation A, B, or C) on behalf of Scyber's originated traffic.
- Scyber ensures that its platform configuration correctly passes verified Caller ID and customer information to the upstream provider to facilitate accurate attestation.

3. Call Analytics and Traffic Blocking

As required by FCC rules to disclose analytics systems and third-party vendors, Scyber utilizes the robocall mitigation and call analytics tools integrated into our upstream provider's network

(SkySwitch/BCM One).

- **Third-Party Vendors:** Scyber relies on analytics and blocking services implemented at the network level by SkySwitch (which utilizes industry-standard vendors such as Nomorobo and Ribbon Communications Reputation Scoring).
- **Blocking Capabilities:** These analytics systems actively monitor call volumes and routing behavior. The network actively blocks calls that spoof invalid, unallocated, or unassigned NANP numbers, as well as calls originating from numbers identified on reasonable "Do Not Originate" (DNO) lists.

4. "Know Your Customer" (KYC) Procedures

To prevent the origination of illegal robocalls, Scyber has implemented affirmative, effective measures to vet both new and renewing customers:

- **Identity Verification:** Prior to onboarding, all prospective commercial customers must provide verifiable business credentials, including a valid physical address, verifiable contact information, and business identification (e.g., EIN or tax ID).
- **Service Evaluation:** Scyber evaluates the customer's intended use of the voice platform. Customers requesting high-volume automated dialing capabilities, predictive dialers, or short-duration call patterns are subject to heightened scrutiny and/or denial of service.
- **Continuous Monitoring:** Scyber monitors account usage post-activation. Sudden spikes in outbound call volume, abnormally short Call Duration (ALOC), or low Answer Seizure Ratios (ASR) trigger internal reviews to detect potential illegal robocall campaigns.

5. "Know Your Upstream Provider" Procedures

Scyber routes 100% of its voice traffic through its designated upstream provider, SkySwitch. As part of our "Know Your Upstream Provider" policy:

- Scyber verifies that SkySwitch (and its parent entity, BCM One) maintains an active, approved filing in the FCC's Robocall Mitigation Database.
- Scyber continually monitors the Robocall Mitigation Database to ensure our upstream provider has not been de-listed or subject to enforcement actions that would prohibit us from routing traffic through them.

6. Contractual Provisions with End-Users

Scyber's Terms of Service and Acceptable Use Policy (AUP) contain strict, legally binding provisions designed to mitigate illegal robocalling and spoofing:

- **Prohibition of Illegal Activity:** Customers are explicitly prohibited from using Scyber's services to originate illegal robocalls, telemarketing calls that violate the TCPA, or calls using illegally spoofed Caller ID information.
- **Traceback Cooperation:** The AUP requires customers to cooperate promptly with any traceback requests or investigations regarding their traffic.
- **Suspension and Termination Rights:** Scyber reserves the right to immediately suspend

or terminate service, without prior notice or liability, if a customer is found to be originating unlawful traffic, violating the AUP, or failing to respond to a traceback request.

7. Traceback Commitment and Law Enforcement Cooperation

Scyber LLC strictly adheres to FCC traceback requirements. Scyber hereby commits to:

1. **Respond within 24 hours** (fully and comprehensively) to all traceback requests from the Federal Communications Commission (FCC), civil and criminal law enforcement agencies, and the industry traceback consortium (the Industry Traceback Group / ITG).
2. **Cooperate fully** with such entities in investigating, identifying, and stopping any illegal robocallers that attempt to use Scyber's services to originate traffic.
3. Take immediate action to block traffic and suspend the accounts of any end-user found to be the source of illegal robocalls.

Revision and Authorization

<i>Revision</i>	<i>Name</i>	<i>Title</i>	<i>Date</i>
1.0	Eric Parsley	President	02/20/2026