

ROBOCALL MITIGATION PLAN

Greenberry Networks, LLC

FCC Registration Number (FRN): 0023458193

Date: February 28, 2026

I. INTRODUCTION AND PURPOSE

This Robocall Mitigation Plan ("Plan") is submitted by Greenberry Networks, LLC ("Greenberry" or "Provider") to the Federal Communications Commission ("FCC") pursuant to 47 CFR § 64.6305 and the requirements of the TRACED Act. This Plan sets forth the Provider's current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network.

Greenberry Networks, LLC is a small Voice over IP (VoIP) telecommunications company providing SIP-based voice services to retail business and residential customers. Greenberry operates as a voice service provider that originates and terminates calls for its end-user customers, connecting them to the public switched telephone network (PSTN) through upstream carrier partners.

The Provider views these policies and procedures as constituting "reasonable steps" to avoid the origination of illegal robocalls on its network. In addition to following these steps, the Provider commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperating with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

II. PROVIDER INFORMATION

Company Name: Greenberry Networks, LLC

FRN: 0023458193

Provider Type: Voice Service Provider

Role in the Call Chain: Originating and Terminating

Foreign Voice Service Provider: No

III. STIR/SHAKEN IMPLEMENTATION STATUS

Greenberry Networks has not yet fully implemented STIR/SHAKEN caller ID authentication on its network. As a small provider with limited technical and financial resources, the Provider is currently working toward implementation and acknowledges this as an ongoing priority.

At this time, the Provider's upstream carrier partners provide STIR/SHAKEN authentication for calls transiting their networks. While the Provider recognizes that reliance on upstream providers for STIR/SHAKEN signing does not satisfy its own independent obligation, the Provider is actively pursuing the following steps toward direct implementation:

1. Obtaining a Service Provider Code (SPC) token from the STI Policy Administrator (iconectiv) to enable direct STIR/SHAKEN signing.
2. Acquiring a STIR/SHAKEN certificate from an authorized Certificate Authority.
3. Configuring STIR/SHAKEN signing capabilities within the Provider's switching platform, which natively supports the STIR/SHAKEN protocol.
4. Testing and validating call signing to ensure proper attestation levels (A, B, or C) are applied based on the Provider's knowledge of the calling party and their authorization to use the originating telephone number.

Pending full STIR/SHAKEN implementation, the Provider relies on the robocall mitigation practices detailed in this Plan to prevent the origination of illegal robocalls on its network.

IV. KNOW YOUR CUSTOMER (KYC) PRACTICES

The Provider maintains rigorous Know Your Customer procedures as a primary means of preventing illegal robocall activity. Given the Provider's small customer base, the Provider has direct personal knowledge of and relationships with each of its customers. This small scale enables a level of customer vetting and oversight that larger providers cannot practically achieve.

Before provisioning service for any new customer, the Provider performs the following verification steps:

- Verification of the customer's identity, including the legal name of the individual or business entity requesting service.
- Collection and verification of the customer's physical business location or residential address.
- Verification of a valid contact telephone number and email address for the customer.
- For business customers, verification of the nature of the customer's business and the intended use of the voice services being provisioned.
- Confirmation that the customer has a legitimate need for the telephone numbers being assigned and is authorized to use those numbers.
- Assessment of the customer's expected call volume and calling patterns to establish a baseline for future monitoring.

The Provider does not provide service to high-volume call centers, auto-dialers, or any customers whose primary business purpose involves mass outbound calling campaigns. The Provider's customer base consists of retail business and residential customers with standard voice communication needs.

V. TELEPHONE NUMBER VALIDATION PRACTICES

The Provider validates that each customer is authorized to use the telephone numbers assigned to their account. The Provider assigns telephone numbers directly to customers from number blocks obtained through authorized sources and maintains records of all number assignments.

When a customer ports a telephone number to the Provider's network, the Provider verifies the customer's authorization to use that number through the standard Local Number Portability

(LNP) process, including verification of the customer's identity and existing account with the losing carrier.

The Provider configures its systems to ensure that customers can only originate calls using caller ID numbers that have been validated and authorized for their account. The Provider's platform is configured to restrict outbound caller ID presentation to numbers assigned to or authorized for each customer.

VI. CALL DETAIL RECORD (CDR) MONITORING AND TRAFFIC ANALYSIS

The Provider monitors the usage of its network and examines call detail records (CDRs) on a recurring basis for the purpose of detecting suspicious call activity and calling patterns that may be indicative of illegal robocalling. The Provider's monitoring practices include attention to the following indicators:

- Higher than normal subscriber traffic volume, including large bursts of traffic in small timeframes or inconsistent volumes of traffic (spikes in usage) relative to the customer's established baseline.
- Originating calls of unusually short duration and low call completion percentages, which may indicate automated dialing of invalid or uninterested numbers.
- Originating calls with sequential called-to-number dialing patterns, which are characteristic of automated dialing systems.
- Calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator (NANPA).

Given the Provider's small customer base, the Provider has detailed familiarity with the normal calling patterns and expected usage of each customer account, which enhances the Provider's ability to promptly identify anomalous activity.

VII. RESPONSE TO SUSPECTED ILLEGAL ROBOCALLING

When network usage patterns consistent with illegal robocalls are detected, or the Provider otherwise suspects illegal robocalling or caller ID spoofing is taking place on its network, the Provider will take the following actions:

5. Immediately investigate to identify the party originating the suspicious calls.
6. Contact the customer to determine whether the calling activity is legitimate and authorized.
7. Verify that the caller ID being presented matches numbers authorized for the customer's account.
8. If illegal robocalling is confirmed or strongly suspected, immediately suspend or terminate the offending customer's ability to originate calls on the Provider's network.
9. Report the incident to the appropriate authorities, including the FCC and the Industry Traceback Group, as applicable.
10. Preserve all relevant call detail records and account information for use in any subsequent investigation.

VIII. CONTRACTUAL PROVISIONS

The Provider is in the process of updating its customer service agreements to include explicit provisions prohibiting the use of the Provider's network for illegal robocalling, caller ID spoofing, or any other unlawful telecommunications activity. These contractual provisions will include:

- A clear prohibition on the use of the Provider's services to originate illegal robocalls, as defined under the Telephone Consumer Protection Act (TCPA) and FCC regulations.
- A prohibition on caller ID spoofing with the intent to defraud, cause harm, or wrongfully obtain anything of value, as prohibited by the Truth in Caller ID Act.
- A requirement that customers cooperate with any traceback investigation conducted by the Provider, the FCC, law enforcement, or the ITG.
- The Provider's right to immediately suspend or terminate service if a customer is found to be originating illegal robocalls or engaging in caller ID spoofing.
- A requirement that customers comply with all applicable federal and state telecommunications laws and regulations.

IX. TRACEBACK COOPERATION

The Provider commits to fully cooperating with traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG). The Provider has designated a single point of contact for receiving and responding to all traceback requests:

Traceback Point of Contact: Josh Horton

Title: Owner / Managing Member

Email: josh@greenberrynetworks.com

Phone: 417-365-0070

Upon receipt of a traceback request, the Provider will promptly identify the upstream provider from which a suspected illegal robocall entered its network, or identify the customer account from which the call originated. The Provider will respond to traceback requests as expeditiously as possible and in no event later than 24 hours after receipt of the request.

X. ONGOING COMMITMENT AND PLAN UPDATES

The Provider is committed to continuously improving its robocall mitigation efforts. The Provider will review and update this Plan as necessary to reflect changes in its operations, technology, customer base, or applicable FCC rules and regulations. The Provider will update its RMD filing within 10 business days of any material changes to the information contained in this Plan.

The Provider acknowledges its obligation to recertify its RMD filing annually by March 1 of each year and commits to timely compliance with this requirement.

CERTIFICATION

I certify that the information contained in this Robocall Mitigation Plan is accurate, true, and correct, and that Greenberry Networks, LLC is committed to implementing and following the practices described herein.

Josh Horton Owner / Managing Member

Greenberry Networks, LLC

Date: __02/28/2026_____