



Robocall Mitigation Program

Effective Date: 01/01/2026

Last Reviewed: 01/01/2026

Filed pursuant to 47 CFR § 64.6305(a)

1. PURPOSE AND SCOPE

Network Computing Solutions ("the Company") is a small voice service provider offering hosted/cloud VoIP services to business customers, operating as a reseller of upstream carrier services with fewer than 1,000 subscriber lines. This Robocall Mitigation Program ("Program") is established pursuant to 47 CFR § 64.6305(a) and describes the reasonable steps the Company takes to avoid originating illegal robocall traffic on its network.

As a provider with fewer than 100,000 subscriber lines, the Company qualifies for the STIR/SHAKEN implementation exemption under 47 CFR § 64.6304(b). The Company has not implemented STIR/SHAKEN but is committed to mitigating illegal robocall traffic through the measures described herein.

2. CUSTOMER ONBOARDING AND VETTING

The Company maintains a formal onboarding process for all new business customers, which includes:

- **Identity Verification:** All prospective customers must provide valid business identification, including legal business name, address, and contact information prior to service activation.
- **Acceptable Use Policy (AUP):** All customers are required to review, acknowledge, and agree to the Company's Acceptable Use Policy, which explicitly prohibits use of the Company's network to originate illegal robocalls, spoofed calls, or any calls that violate the TCPA, Truth in Caller ID Act, or applicable federal or state law.
- **Service Agreement / Terms of Service:** All customers must execute a service agreement that includes provisions allowing the Company to suspend or terminate service for violations of the AUP or applicable law.
- **Use Case Review:** For customers with high call volumes or automated calling needs, the Company reviews the intended use case prior to provisioning service to assess potential for illegal robocall traffic.

3. CALL MONITORING AND ANALYTICS

The Company is a reseller of upstream carrier services and relies on its upstream carrier's network monitoring tools and analytics to assist in detecting unusual or suspicious call patterns. The Company:

- Maintains an active relationship with its upstream carrier and monitors alerts, flags, or notifications provided regarding anomalous traffic originating from the Company's customer base.
- Promptly investigates any traffic flagged by the upstream carrier and takes appropriate action, including customer notification, suspension, or termination of service.
- Periodically reviews call volume and usage patterns for its business customers to identify any significant or unexplained changes in call behavior.

4. RESPONSE TO TRACEBACK REQUESTS

Network Computing Solutions is committed to cooperating fully with traceback requests from the Commission, law enforcement, and the industry traceback consortium (USTelecom's Industry Traceback Group). The Company will respond to all traceback requests fully and within 24 hours of receipt. Traceback requests should be directed to:

Traceback & Compliance Contact

Todd Fannin — Manager of Technical Operations

Email: tfannin@ncsmidwest.com

5. ENFORCEMENT AND REMEDIATION

Upon identification of a customer originating illegal robocall traffic, the Company will:

- **Immediate Investigation:** Review all available call records and usage data related to the flagged customer.
- **Customer Notification:** Contact the customer to inform them of the suspected violation and demand immediate cessation of illegal calling activity.
- **Suspension or Termination:** If illegal activity is confirmed or the customer fails to remediate, the Company will suspend or terminate service in accordance with its Terms of Service and AUP.
- **Cooperation with Authorities:** The Company will cooperate fully with law enforcement, the FCC, and the industry traceback consortium in any related investigation.
- **Upstream Carrier Notification:** The Company will notify its upstream carrier of confirmed or suspected illegal traffic as appropriate.

6. UPSTREAM CARRIER OBLIGATIONS

As a reseller, the Company acknowledges its responsibility to ensure that its upstream carrier is registered in the FCC's Robocall Mitigation Database. The Company will verify upstream carrier registration prior to and during the term of any reseller agreement, and will include robocall mitigation compliance obligations in upstream carrier agreements where applicable.

7. EMPLOYEE AWARENESS

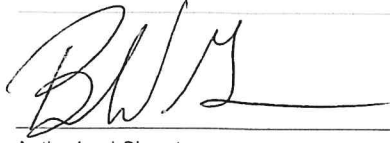
The Company will ensure that relevant staff are aware of this Program and their responsibilities, including familiarity with the AUP, understanding of how to receive and respond to traceback requests, and awareness of FCC rules governing illegal robocalls and spoofing.

8. PROGRAM REVIEW AND UPDATES

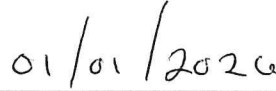
This Program will be reviewed at least annually and updated as necessary to reflect changes in the Company's operations, applicable FCC rules, or industry best practices. Updates will be reflected in the Company's filing in the FCC Robocall Mitigation Database.

9. CERTIFICATION

Network Computing Solutions certifies that this Robocall Mitigation Program reflects the reasonable steps it is taking to avoid originating illegal robocall traffic, consistent with 47 CFR § 64.6305(a), and that the Company is committed to full cooperation with traceback requests and law enforcement inquiries.



Authorized Signature



Date

Bryce Garner

Printed Name

Owner / CEO

Title