



Robocall Mitigation Program

Last Updated: 03/2026

Company Overview

Acuity Technology Solutions Inc.
439 Jevlan Drive
Woodbridge, ON. L4L 8A9

Our company provides VoIP telecommunications services to business customers and utilizes upstream carrier partners to route calls to the public switched telephone network (PSTN). We are a foreign voice service provider based in Ontario, Canada. Our operations fall under the requirements outlined in 47 CFR § 64.6305 for providers that originate voice traffic but rely on upstream carriers to implement STIR/SHAKEN authentication.

STIR/SHAKEN call authentication is implemented by our upstream carrier partners prior to calls entering the United States PSTN. Our network does not independently sign calls but we take reasonable steps to ensure that traffic originating from our network complies with applicable caller identification and anti-spoofing requirements.

Robocall Mitigation Program

We maintain a robocall mitigation program designed to prevent the origination or transmission of illegal robocalls and caller ID spoofing on our network. This program includes reasonable practices and safeguards consistent with 47 CFR § 64.6305(c) to reduce the risk that our services are used to originate or transmit unlawful robocall traffic.

Customer Vetting, KYC, and Identity Verification

Prior to provisioning service, we perform reasonable due diligence to verify the identity of customers and the legitimacy of their intended use of our voice services. As part of our Know Your Customer (KYC) process, we collect and verify information sufficient to identify the customer and assess potential risk associated with their use of telecommunications services.

These procedures may include:

- Verification of legal business name and registration information
- Collection and validation of physical business address and contact details
- Verification of authorized representatives responsible for the account
- Review of the customer's intended use of voice services



- Risk assessment for high-volume or automated outbound calling use cases

Service may be denied, restricted, or subject to additional review if there is a reasonable risk that the service could be used to originate illegal robocalls or facilitate caller ID spoofing.

Caller ID Authentication and Validation

Our network enforces caller ID policies intended to prevent caller ID spoofing and misleading caller identification information. Outbound caller ID is restricted to numbers assigned to or authorized for use by the customer. Invalid, non-dialable, or obviously fraudulent caller ID values may be blocked or rewritten. Where applicable, caller ID numbers are normalized to standard E.164 formatting prior to delivery to upstream carriers.

Traffic Monitoring and Abuse Detection

We monitor network traffic patterns and call detail records (CDRs) for indicators of suspicious or abusive calling activity. Monitoring may include analysis of call detail records, review of high call-per-second (CPS) rates, abnormal call duration patterns, unusually high call volumes, and other traffic anomalies that may indicate illegal robocall activity.

Network safeguards may include rate limiting controls, traffic anomaly detection, and other operational monitoring designed to identify potential robocall campaigns or abusive calling behavior.

Where suspicious activity is detected, we may investigate the originating customer account, review associated CDR data, and take appropriate corrective action including temporary rate limiting, suspension of outbound calling, or further investigation as required.

Acceptable Use Policy

All customers must comply with our Acceptable Use Policy (AUP) governing the use of our telecommunications services. The AUP expressly prohibits the use of our services for unlawful robocalling, caller ID spoofing, fraudulent communications, harassment, or any activity that violates applicable telecommunications laws and regulations.

Customers are prohibited from:

- Originating illegal robocalls
- Transmitting misleading or falsified caller identification information
- Using automated dialing systems in violation of applicable laws
- Engaging in traffic pumping, fraudulent traffic generation, or other abusive calling practices



Violation of the Acceptable Use Policy may result in immediate suspension or termination of service and may be reported to upstream carriers or appropriate authorities where required.

Enforcement and Mitigation Actions

If potentially abusive or unlawful calling activity is identified, we may take mitigation actions including investigation of the account, temporary suspension of outbound calling privileges, or termination of service for confirmed violations. These actions are intended to prevent our network from being used to originate or facilitate illegal robocalls.

Upstream Carrier Coordination

Our network interconnects with upstream carriers that implement STIR/SHAKEN authentication prior to calls entering the PSTN. We cooperate with these carriers in identifying and mitigating potentially abusive traffic originating from our network and may provide information necessary to assist in mitigation efforts.

Traceback Cooperation

We commit to responding fully and within 24 hours to traceback requests from the Federal Communications Commission, law enforcement agencies, and the Industry Traceback Group. We will cooperate with these entities to identify the source of suspected illegal robocalls and take appropriate steps to prevent further transmission of such traffic.

Regulatory Compliance Statement

In the past two years, neither the filing entity nor any entity with shared ownership, management, directors, or control has been the subject of any formal action or investigation by the Commission, law enforcement, or any regulatory agency related to allegations of transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or caller ID spoofing. Additionally, there have been no findings of deficiencies in our Robocall Mitigation Database certification or mitigation program description. We remain fully compliant with all regulatory requirements and are committed to upholding the highest standards of integrity in preventing illegal robocall activities.

Ongoing Compliance

Our robocall mitigation program is reviewed periodically and updated as necessary to address evolving regulatory requirements and industry best practices for preventing illegal robocalls and caller ID spoofing. Personnel responsible for network operations are expected to comply with



this program and take reasonable steps to ensure that our network is not used to facilitate unlawful robocall activity.

Closing Statement

This robocall mitigation program is maintained in accordance with the requirements of 47 CFR § 64.6305 and reflects the reasonable steps implemented by our organization to prevent the origination or transmission of illegal robocalls and caller ID spoofing. We maintain appropriate internal controls to ensure compliance with these requirements and will update our Robocall Mitigation Database filing within the timeframes required by the Federal Communications Commission if any material changes occur to our mitigation practices, network architecture, or certification status. Our organization remains committed to cooperating with regulators, law enforcement agencies, and the Industry Traceback Group to prevent abuse of telecommunications networks and to uphold the integrity of the voice communications ecosystem.

Authorization

This robocall mitigation program description is certified as accurate and complete to the best of our knowledge and reflects the policies and procedures implemented by our organization to prevent illegal robocalls and caller ID spoofing.

Authorized Representative:

Michello Foster

President

Acuity Technology Solutions Inc.