



Version 3 — February 2026

Robocall Mitigation Plan for Tridacom IT Solutions Inc. DBA ReliaRing ("Tridacom")

Tridacom IT Solutions Inc. ("Tridacom"), doing business as ReliaRing, is a voice service provider committed to preventing illegal robocalls from originating on its network. Tridacom is committed to responding fully and within 24 hours to all traceback requests from the Federal Communications Commission (FCC), law enforcement, and the Industry Traceback Consortium (formerly the US Telecom Industry Traceback Group). Tridacom shall cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls and will designate a single point of contact for each traceback request in order to expedite the process.

ROBOCALL MITIGATION DATABASE STATUS

All calls on Tridacom's network are subject to this Robocall Mitigation Plan. Tridacom's existing certification in the Robocall Mitigation Database has not been removed by the Commission, nor has Tridacom been prohibited from filing in the Robocall Mitigation Database.

STIR/SHAKEN IMPLEMENTATION

Tridacom has fully implemented the STIR/SHAKEN caller-ID authentication framework across its network. Specifically:

- Tridacom is registered with the STIR/SHAKEN Policy Administrator (STI-PA) and holds its own Service Provider Code (SPC) token.
- Tridacom uses digital certificates issued by an STI-PA-approved Certificate Authority to sign originating calls.
- All calls originating on Tridacom's network are authenticated with full attestation (Level A) where Tridacom is the originating provider, in compliance with 47 CFR § 64.6301.
- Tridacom's STIR/SHAKEN implementation is maintained and updated to remain compliant with evolving FCC requirements and industry standards.

ACTIONS TAKEN BY TRIDACOM TO DETECT ORIGINATING ROBOCALL TRAFFIC

- A. Tridacom limits the daily and monthly dollar amounts of calls placed per customer account, with limits set based on the type of customer.
- B. Tridacom's network is monitored for fraud and fraudulent activity by automated systems that run continuously to detect suspicious patterns. Upon detection, alerts are sent to the Network Operations team for review. The Network Operations team also receives and processes information from upstream and downstream providers. If any potentially fraudulent activity is detected, Tridacom acts as quickly as possible to reject such traffic

through blocks and notify the customer of the fraudulent activity.

- C. Tridacom monitors call thresholds at all times. System logs are reviewed regularly to identify suspicious calling activities, including unusual call volumes, short-duration call patterns, and anomalous destination patterns.
- D. Tridacom employs STIR/SHAKEN authentication on all originating calls as described above, providing cryptographic verification of caller identity and an additional layer of robocall detection.

ACTIONS TAKEN BY TRIDACOM TO PREVENT ILLEGAL ORIGINATING ROBOCALL TRAFFIC

- A. Tridacom only allows its customers to present an ANI (Automatic Number Identification) that is registered to them. If a request is received for an ANI that is not registered to the end user, it will be overridden with the default ANI on the customer's account.
- B. Procedures are in place to confirm the identity of new commercial customers by collecting information such as physical business location, contact person(s), state and country of incorporation, Federal Tax ID, general nature of the customer's business, names of all officers and directors of the business, public research into the history of the company including public complaint data, other business reputation data, officers/directors, and any other business in which they may be involved.
- C. Tridacom's Acceptable Use Policies (AUP), Terms and Conditions, and Terms of Service are contained in the service contracts with Tridacom's customers and are also published on its website. These documents explicitly address Tridacom's prohibition of illegal robocalling.
- D. Each new customer of Tridacom must agree to a Service Contract. Within the Service Contract is incorporated a reference to the AUP under which the customer is obligated. The customer must sign a Service Contract, or they will not be permitted to use Tridacom's service. Among other things, Tridacom's AUP and service contracts prohibit:
 - a. providing deceptive or false information about the identity of the sender or the origin of a message or phone call;
 - b. violating any applicable local, state, or Federal law;
 - c. violating any applicable industry acceptable guidelines;
 - d. using Tridacom's service to engage in or in connection with fraudulent activities;
 - e. Tridacom's contractual terms with subscribers specify Tridacom may take action, up to and including suspension or termination of service, for violation of the AUP or Terms of Service.
- E. Tridacom will maintain participation in the FCC Robocall Mitigation Database (RMD) and will adhere to its guidelines and best practices.

HOW TRIDACOM INVESTIGATES SUSPICIOUS ACTIVITY

Tridacom regularly examines and analyzes its traffic composition. If the analysis indicates the presence of likely illegal robocalling, the Network Operations team is alerted, and they follow defined procedures for investigating the customer who is generating the suspicious traffic.

The procedures include but are not limited to:

- Checking recent and past call detail records and benchmarking them against expected trends
- Checking recent and past account activity and purchase history
- Reviewing support tickets and any other customer account notes
- Investigating if any system issue generates the abnormal traffic patterns
- Verifying that the call originating path is valid
- Blocking traffic until the investigation can be completed
- Contacting the customer to understand their particular use case and validate that the activity belongs to that customer

CALL BLOCKING

Tridacom shall implement any Do Not Originate request it receives from the Industry Traceback Consortium. In addition, any suspicious activity may be blocked pending completion of an internal investigation by the Tridacom Network Operations team.

CONTACT INFORMATION FOR ROBOCALL MITIGATION OR SUSPICIOUS ACTIVITY

If suspicious activity has been reported or identified on Tridacom's network, it can be reported to the following:

Tridacom Network Operations Centre (NOC)

10215 178 Street NW
Edmonton, AB T5S 1M3
Canada

Toll Free: +1 877.631.0058
Email: noc@tridacom.com

ENFORCEMENT HISTORY DISCLOSURE

Tridacom has not been subject to any enforcement action, investigation, or warning by the FCC, state regulatory agency, or law enforcement related to robocalling, illegal call traffic, or violations of the Telephone Consumer Protection Act (TCPA) or Truth in Caller ID Act.

PRINCIPALS, AFFILIATES, AND SUBSIDIARIES

Tridacom IT Solutions Inc. is wholly owned by its principal:

Michael Somerville, President

30 College Park Close
Red Deer, AB T4P 0M7
Canada

Tridacom IT Solutions Inc. has no parent company, affiliates, or subsidiaries that are voice service providers filing separately in the Robocall Mitigation Database.

UPDATES TO ROBOCALL MITIGATION PLAN

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. Tridacom will monitor industry best practices and continuously improve its internal processes to ensure this plan and its systems adapt to ever-changing issues.

When any processes or procedures change, Tridacom shall republish this plan to its employees, consultants, and contractors and file such an update to the FCC Robocall Mitigation Database.

CORES COMPLIANCE

Tridacom commits to maintaining current and accurate information in the FCC's Commission Registration System (CORES). Tridacom will update its CORES registration within 10 business days of any change to its entity name, address, contact information, or other required data, in accordance with 47 CFR § 1.8002.