

International Telnet Inc. Robocall Mitigation Plan

I. Background

The Federal Communications Commission (FCC) requires voice service providers to file certifications and robocall mitigation plans in the Robocall Mitigation Database (RMD). These plans must outline reasonable steps to prevent the origination of illegal robocall traffic. The provider must also commit to responding to all traceback requests from the Commission, law enforcement, and the industry traceback consortium within 24 hours.

While the FCC's rules do not have a single definition for "robocall," International Telnet Inc. focuses its efforts on two types of unlawful calls that violate the TCPA: calls made with an artificial or prerecorded voice, or with an automatic telephone dialing system, and calls with intentionally misleading or inaccurate caller ID information. The Commission has stated that a mitigation program is sufficient if it includes detailed practices that can reasonably be expected to significantly reduce a provider's origination or carriage of illegal robocalls.

II. Know Your Customer (KYC) Standards

1. Objective

As part of its Risk Management and Compliance Program, International Telnet Inc. has implemented this Customer Identification Program (CIP) to prevent its services from being used for illegal or fraudulent activities. This program is designed to form a reasonable belief that we know the true identity of our customers by verifying key information for each business entity and its primary contact.

2. Customer Identification Program (CIP)

International Telnet Inc. serves business customers and collects and verifies identifying information for each entity before providing service. All customers are onboarded through an enrollment process managed and reviewed by our staff.

2.1. Information Collected

For each prospective business customer, we collect the following minimum information:

- Legal Business Name and any "Doing Business As" (DBA) names.
- Federal Employer Identification Number (EIN) or equivalent tax identification number (for all new customers onboarded from September 2025 onward).
- Physical address of the principal place of business (P.O. Boxes are not acceptable).
- Company email, primary phone number, and official website domain.
- State or country of incorporation/registration.
- Full name, title, and contact information for the primary contact person(s).

- A copy of a government-issued photo ID (e.g., driver's license or passport) for the primary contact person.
- A description of the customer's intended use of the service, including the nature of their business, and the purpose of any calling campaigns.

2.2. Verification Procedures

Information collected during onboarding is verified using a combination of documentary and non-documentary methods before account activation. These steps include:

- **Verify the Business Entity:** Cross-referencing the business name and other identifiers with the relevant Secretary of State or other national business registry to confirm the company is in good standing.
- **Verify EIN:** For customers onboarded from September 2025, using the provided EIN as a key identifier for cross-referencing public records and confirming the entity's legitimacy.
- **Verify Primary Contact's Identity:** Reviewing the government-issued photo ID provided by the primary contact to ensure it appears legitimate and that the name matches the information provided during enrollment.
- **Verify Physical Address:** Using online maps and public records to confirm the legitimacy of the physical business address.
- **Assess Intended Use:** Reviewing the customer's stated business purpose and website to ensure it aligns with our acceptable use policy.

2.3. Use of Third-Party Analytics and Verification

International Telnet Inc. currently conducts all customer verification using the internal, documentary, and non-documentary methods described above. We do not currently employ a third-party vendor for these processes. This decision is reviewed annually as part of our risk management assessment.

III. Acceptable Use Policy (AUP)

All customers agree to comply with International Telnet Inc.'s Acceptable Use Policy as part of the onboarding process. The AUP prohibits a number of activities, including but not limited to:

- Engaging in any illegal, abusive, fraudulent, or misleading activities.
- Engaging in any unsolicited advertising, marketing, or other unlawful activities that violate applicable laws, such as the Telephone Consumer Protection Act (TCPA).
- Creating a false identity, a forged email address or phone number, or otherwise attempting to mislead others as to the origin of a message or call.

International Telnet Inc. can suspend or terminate services for any AUP violation.

IV. Telephone Number Authorization and STIR-SHAKEN

International Telnet Inc. has fully implemented the STIR/SHAKEN authentication framework across its entire network. All calls for which it is the originating carrier are compliant with the relevant regulations (iConectiv STIPA registration #102378). In addition, International Telnet Inc. has procured a STIR/SHAKEN certificate from Telonium to allow for token generation.

Customers can only use telephone numbers they have subscribed to from International Telnet Inc. or numbers they can verify have been assigned to them from other carriers.

V. Proactive Network Monitoring and Analytics

International Telnet Inc. has monitoring and reporting systems to analyze network traffic for suspicious patterns that may be associated with illegal robocalls or other unlawful usage. The company uses a variety of criteria to assess traffic, including data related to short-duration calls, call-failure ratios, and other calling patterns.

If International Telnet Inc. detects a pattern consistent with illegal robocalls, it takes prompt action to identify the responsible party. Once detected, the company blocks any further traffic associated with that suspicious activity.

VI. Commitment to Timely Traceback Responses and Cooperation

International Telnet Inc. commits to responding fully and in a timely manner—within 24 hours—to all traceback requests from the Commission, law enforcement, and the industry traceback consortium. The company will cooperate with these entities in investigating and stopping any illegal robocallers that use its service. International Telnet Inc. will dedicate sufficient resources to provide timely and complete responses to these requests.