

Robocall Mitigation Plan

AccessLine Communications Corporation d/b/a Voice Telco Services

AccessLine is dedicated to stopping illegal calls from originating in AccessLine's network and monitoring the calls coming into its network, in accordance with FCC regulations. This document defines AccessLine's Robocall Mitigation Plan.

Overview

The Federal Communications Commission ("FCC") requires that all providers certify in the Robocall Mitigation Database that they have instituted a Robocall Mitigation program designed to ensure that they are not originating illegal robocalls.

AccessLine Communications Corporation ("AccessLine") d/b/a Voice Telco Services ("Voice Telco Services") is a wholly owned subsidiary of Intermedia.net, Inc. ("Intermedia"). AccessLine's Robocall Mitigation Plan is designed to prevent the origination of robocalls on AccessLine's network and is modeled on the FCC's best practices focused on subscriber vetting, telephone number validation and ongoing robocall mitigation. AccessLine will continue to monitor and, as appropriate, incorporate improved processes and best practices into its Robocall Mitigation Plan.

Know Your Customer Procedures

AccessLine is a Voice Service Provider with STIR/SHAKEN obligation originating calls and serving end-users. As such, AccessLine's service is marketed and sold to the small and medium-sized business ("SMB") market through both retail and wholesale channels. Regardless of sales channel, the sales process involves vetting of new customers/subscribers, including the following:

- All new subscribers must provide a valid credit card or business credentials verification (e.g., Dunn and Bradstreet check) that must match the business address where service is to be installed.
- Our sales team must verify customers credit card is not a gift card or prepaid card and is indeed connected to a bank account.
- Each new subscriber's business address is validated as a business location and must align with the billing or credit card address.
- Test charges are applied to accounts to help determine the legitimacy of the subscriber's business.
- All new subscribers are checked against AccessLine's historical database of violators of AccessLine's Acceptable Use Policy.
- AccessLine also empowers its sales and support team to flag suspicious customers for fraud review by an independent team of AccessLine employees. The fraud review team performs various activities, including:
 - Verifying that the business address is owned by the subscriber;
 - Verifying the business against Dunn and Bradstreet data;
 - Verifying the business address, shipping address and billing address correlate to the stated business;
 - Verifying that subscribers and/or contacts for the business can be associated with the business through web searches (e.g., LinkedIn, Better Business Bureau, social media);
 - Confirming that the email domain and company website domain match and are valid;
 - Verifying the owner of the email/web domain;
 - Confirming the lease or business license for the applicable property address; and

- Reviewing purchase and usage patterns typical of the SMB market.

Any potential customer/subscriber that fails AccessLine's vetting process is rejected, and service is not activated.

Master Service Agreement (MSA)

Purchasers that pass AccessLine's vetting process must also agree to a Master Service Agreement ("MSA"). All customers are required to sign or electronically accept an MSA, which incorporates a Product Schedule that explicitly prohibits use of the service for Robocalling purposes and gives AccessLine the right to terminate service if this prohibition is violated.

SIP End Point Verification

Once a purchaser has been vetted and has agreed to the MSA, AccessLine verifies the SIP endpoints that are allowed to access its network. All devices used to originate a call on the AccessLine network are verified by:

- username/password;
- IP address; or
- MAC address and device type.

Devices that cannot be verified are not granted access to AccessLine's service.

Telephone Number Validation

A Telephone Number (TN)-based caller identity is defined as the originating phone number included in call signaling. The TN is used to identify the caller for call screening purposes and is uniquely associated with a subscriber.

AccessLine is able to provide new TNs obtained from one of its underlying carriers and also allows customers to import (port) TNs for use with AccessLine's service. AccessLine uses industry standard practices to port subscriber-owned phone numbers into the AccessLine network, which include the following verification procedures:

- Porting of a number into the AccessLine network is not allowed until the customer/subscriber passes AccessLine's vetting process;
- AccessLine follows industry standard carrier processes to verify number ownership by obtaining a signed Letter of Authorization (LOA) and/or certification from the marketing agent that they are working with an authorized end user;
- AccessLine requests a correlated bill copy with proof of telephone number ownership that aligns with the LOA; and
- AccessLine's underlying carriers then verify the provided documentation against losing carrier systems before assigning the telephone number to us.

AccessLine manages TNs used by its subscribers, tracks these numbers in its inventory system, and monitors the assignment of these numbers.

Retail/Wholesale SIP Trunking Service

SIP Trunking service allows a customer to deliver calls to AccessLine's network with any originating calling party's TN. However, AccessLine's MSA and associated product documentation require that the customer must own and have the right to use the telephone number that is used as the originating calling party's TN. All traffic from AccessLine's SIP Trunking service is monitored and is subject to the terms of the MSA. AccessLine will terminate customers that violate the MSA or fails to adhere to US Telco telecom and ITG standards.

Ongoing Fraud and Robocall Mitigation

AccessLine maintains a comprehensive robocall mitigation program focused on proactively monitoring, identifying, and preventing illegal or fraudulent calling activity across its network. The following controls, processes, and procedures are in place:

- AccessLine actively cooperates with the USTelecom Industry Traceback Group (ITG) and participates in both traceback and trace-forward investigations. Documented procedures are in place, and the support team is trained to respond promptly and effectively to ITG inquiries.
- AccessLine works closely with its underlying carriers to identify, investigate, and mitigate robocalls originating from its network.
- AccessLine operates a sophisticated, real-time automated monitoring system designed to detect suspicious calling patterns, including robocalling behaviors. Flagged calls are escalated to the robocall mitigation team for further analysis and action.
- Access to the network via SIP user agents is tightly controlled using multiple criteria, including geographic restrictions, IP allow/block lists, device type validation, and SIP registration signatures.
- Customers are restricted to using only telephone numbers provisioned by AccessLine as their outbound Caller Line ID (CLI), unless explicitly approved through a formal vetting process.
- For non-AccessLine numbers, customers must complete a verification process that includes:
 - Submission of documentation (e.g., phone bill) proving number ownership
 - Live verification via a support-led call with security validationOnly after successful verification will the number be authorized for outbound CLI use. Customers are not permitted to self-configure unverified caller IDs.
- AccessLine enforces the ITG Do Not Originate (DNO) list. Any outbound calls using DNO-listed numbers are automatically blocked, logged, and reviewed.
- Sales teams are trained to identify indicators of fraudulent accounts during onboarding. This includes recognizing suspicious patterns and escalating potential risks. The robocall mitigation team provides continuous feedback on emerging fraud trends, and periodic refresher training is conducted.
- AccessLine maintains a centralized database of fraud and robocall incidents, capturing key attributes such as account details, payment information, business identity, phone numbers, IP addresses, email addresses, and campaign types. This data is used for proactive fraud detection, cross-account correlation, and risk scoring of new and existing customers.

Enforcement and Remediation

All suspected fraud and robocalling activity, along with associated customer accounts, is reviewed by the robocall mitigation team. If a customer is found to be in violation of AccessLine's Acceptable Use Policy, Fair Use Policy, or applicable telecommunications regulations:

- The customer will be notified and required to immediately cease the offending activity
- AccessLine may suspend or terminate the account
- Terminated customers are added to an internal blacklist to prevent re-entry into the network

Traceback and Enforcement Cooperation

AccessLine actively cooperates with the traceback community including the FCC, local, state and federal law enforcement, and The Industry Traceback Group (ITG) to investigate and stop illegal robocalls. Our 24/7 Network Operations Teams is trained to process and respond to traceback requests, from the ITG, within the required 24 hour response period.

STIR/SHAKEN Implementation

AccessLine has implemented the requirements of STIR/SHAKEN and support STIR/SHAKEN requirements for all calls in and out of the AccessLine network.

Role in the Call Chain

AccessLine is a voice service provider with a STIR/SHAKEN implementation obligation serving end users. AccessLine originates calls for our subscribers, has implemented steps to limit robocalls from originating from our network and fully cooperates with downstream carriers to identify and block any robocalls originated from our network.

Plan Updates

This Robocall Mitigation Plan must evolve, as must industry best practices, to respond to the constantly changing practices and techniques that are used to engage in, as well as detect and prevent, illegal robocalling. AccessLine will continue to monitor industry best practices and improve its internal processes to ensure that this Robocall Mitigation Plan and AccessLine's systems adapt to this ever-changing issue.

In the event of any material change to this Robocall Mitigation Plan, AccessLine will republish it to employees, consultants and contractors, as applicable, and submit such update to the FCC's Robocall Mitigation Database.