

ROBOCALL MITIGATION PLAN

FEDERAL COMMUNICATIONS COMMISSION

Ameratech, LLC

Revised February 2026

Regulatory Basis

The Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) requires voice service providers to implement STIR/SHAKEN authentication on Session Initiation Protocol (“SIP”) traffic on carrier networks as well as to implement a Robocall Mitigation Plan covering non-SIP Time Division Multiplexing (“TDM”) traffic. Ameratech, LLC (“Ameratech”) submits this Robocall Mitigation Plan to the Robocall Mitigation Database describing and confirming practices, policies, and procedures to mitigate unlawful robocalling, which include the following:

- (1) Ameratech’s specific reasonable steps to avoid originating illegal robocall traffic as part of this Robocall Mitigation Plan;
- (2) Ameratech’s commitment to respond fully and timely to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers using Ameratech’s service to originate calls;
- (3) Ameratech’s intent to participate in industry tradeshows, groups, or consortiums, working to strengthen efforts to combat unlawful robocalling, and additional call verification and authentication solutions;
- (4) A description of affirmative, effective measures Ameratech takes to prevent new and renewing customers from using Ameratech’s services to originate or route illegal calls;
- (5) A description of Ameratech’s know-your-upstream-provider procedures; and
- (6) A description of the call analytics systems Ameratech uses to identify and block illegal traffic.

About Ameratech

Ameratech (499-A Filer ID: 837756 & OCN: 472L) operates as an intermediate provider (“Intermediate Provider”), neither originating nor terminating calls. As an Intermediate Provider, Ameratech only accepts traffic that has been fully tokenized; Ameratech does not allow untokenized traffic and only offers services to carriers that are in compliance with applicable FCC requirements. Foreign-based carriers are prohibited by Ameratech so as to eliminate first-hop status into U.S. networks. Ameratech requires gatekeepers to authenticate calls prior to passing calls downstream to Ameratech, consistent with the Commission’s rules extending authentication requirements to gateway intermediate providers.

Ameratech operates at all times consistent with the rules, regulations, and Orders of the Federal Communications Commission (“Commission”).

STIR/SHAKEN Obligations for Intermediate Providers

The Commission requires Intermediate Providers to upgrade networks and implement STIR/SHAKEN to authenticate calls in certain situations. Ameratech authenticates calls to verify STIR/SHAKEN compliance and then passes the calls onto the appropriate downstream vendors. In addition, the Commission extends several Robocall Mitigation Database filing requirements to all providers, including without regard to STIR/SHAKEN implementation status. In particular, the Commission requires all providers, including Intermediate Providers and voice service providers that have fully implemented STIR/SHAKEN, to take “reasonable steps to mitigate illegal robocalls” and file certifications along with robocall mitigation plans in the Robocall Mitigation Database. In addition to implementing full STIR/SHAKEN compliance, Ameratech adheres to robocall mitigation practices reasonably expected to significantly reduce the processing or origination of illegal traffic as set forth in this Robocall Mitigation Plan.

Robocall Mitigation Plan

Ameratech utilizes a third-party software-as-a-service switch platform provider called 46Labs Peeredge. In conjunction with this switch platform, Ameratech monitors outbound voice traffic to help control unusual traffic patterns and minimize exposure via alerts and actions in real time, and to help minimize and prevent the origination of illegal robocalls to the best of its abilities.

Ameratech investigates any identified calls to determine whether the caller seeks to originate unlawful robocalls. If Ameratech determines the calls include attempts to originate unlawful robocalls, Ameratech will either warn the customer to cease, block the calling, and/or terminate service consistent with industry standard operating procedures. Ameratech balances any blocking and termination efforts with the goal of preventing the blocking of legitimate calls, particularly those that have a bearing on public safety or health (e.g., school system alerts or law enforcement notifications).

Know Your Customer (KYC)

Ameratech follows the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group. Ameratech currently functions solely as an Intermediate Carrier with no direct-retail end-users and no international customers for which Ameratech would serve as the “first hop” into the United States.

A. Identification of Robocall Risk. Ameratech’s goal through the KYC process remains to identify initially those customers that may engage in the use of robocalls. A “Robocall” means an illegal call using an auto-dialer with a random or sequential telephone number generator that delivers an initial prerecorded message or artificial voice that occurs either (i) for telemarketing

purposes without the called party's prior written consent, or (ii) to a wireless number for any purpose without prior express consent.

B. Customer Screening. From each customer, Ameratech requires the following information, which Ameratech maintains electronically in its records through a standardized KYC form:

- Physical location and address and the telephone number;
- Contact person;
- Contact title
- Place of incorporation (state or country);
- Federal tax identification number;
- FRN number
- RMD number
- OCN number
- Type of customer account (wholesale carrier, intermediate carrier, etc.);
- Nature of customer's business;
- Size of customer's business;
- Whether auto-dialers are used for any purpose; and
- Confirmation that the customer does not operate as a foreign-based carrier (Ameratech prohibits foreign-based customers to eliminate Ameratech's possible status as "first hop into the U.S.").

C. Contractual Obligations. Ameratech's service agreements and contracts require customers to comply with Ameratech's Acceptable Use Policy, which prohibits robocalls and authorizes Ameratech to report suspicious activity when identified. All new customer agreements and renewals incorporate these requirements.

D. Measures to Prevent New and Renewing Customers from Originating Illegal Calls. In compliance with the Commission's expanded content requirements, Ameratech has implemented the following affirmative measures with respect to new and renewing customers:

- **Pre-Activation Screening.** Before activating service for any new customer, Ameratech reviews the prospective customer's KYC form, verifies the customer's business identity and operational history, and confirms consistency with legitimate carrier or wholesale operations.
- **Contractual Acknowledgment.** All new customer agreements require affirmative acknowledgment of and agreement to Ameratech's Acceptable Use Policy, including the prohibition on robocalls and the obligation to cooperate with traceback investigations.

- **Volume and Traffic Pattern Assessment.** Ameratech evaluates expected traffic volumes and patterns at onboarding. Prospective customers requesting unusually high volumes or exhibiting traffic patterns inconsistent with their stated business purpose may be subject to enhanced due diligence, additional documentation requirements, or denial of service.
- **Ongoing Monitoring at Renewal.** At the time of contract renewal, Ameratech reviews the customer's historical traffic patterns, traceback history, and compliance with the Acceptable Use Policy. Ameratech reserves the right to decline renewal or impose additional conditions on customers whose traffic patterns raise compliance concerns.

Know Your Upstream Provider

In compliance with the Commission's directives requiring all providers to describe know-your-upstream-provider procedures, Ameratech has implemented the following measures with respect to the carriers and providers from which Ameratech accepts traffic:

- **Carrier Qualification.** Before entering into a service agreement with any upstream carrier, Ameratech verifies that the carrier maintains an active filing in the Robocall Mitigation Database and has not been the subject of removal by the Commission's Enforcement Bureau. Ameratech only accepts traffic from carriers that are in compliance with applicable FCC requirements, including STIR/SHAKEN authentication.
- **Tokenization Requirement.** Ameratech accepts only fully tokenized traffic. Untokenized traffic from upstream providers remains prohibited. This requirement serves as a threshold check ensuring that upstream carriers have applied STIR/SHAKEN authentication before delivering traffic to Ameratech.
- **Prohibition on Foreign-Based Carriers.** Ameratech prohibits foreign-based carriers from delivering traffic directly to Ameratech so as to eliminate first-hop status into U.S. networks. Ameratech requires gateway providers to authenticate calls prior to passing them downstream.
- **Contractual Protections.** Ameratech's interconnection and service agreements with upstream providers include provisions requiring cooperation with traceback investigations, compliance with applicable robocall mitigation rules, and the right to terminate the agreement in the event of noncompliance.
- **Traffic Monitoring.** Ameratech monitors inbound traffic from upstream providers for anomalies, including unusual call volumes, short-duration calls, and patterns consistent with illegal robocalling. When suspicious traffic patterns are identified, Ameratech works with the upstream provider to investigate and, if necessary, block the offending traffic.
- **Periodic Review.** Ameratech periodically reviews the RMD filings and compliance status of upstream providers to confirm that they remain in good standing with the Commission.

Traceback

Ameratech responds to all traceback requests from the Commission, law enforcement, and the registered traceback consortium, and cooperates with such entities in investigating and stopping illegal robocallers from using Ameratech's service to originate or route calls.

To allow for timely and comprehensive response to traceback requests, Ameratech maintains and will devote sufficient resources to provide prompt and complete records. Ameratech designates the following individual as the single point of contact for receiving all traceback requests:

Ronald LaRoe
President/CEO
Ameratech, LLC
11523 Palmbrush Trl, Ste. 190
Lakewood Ranch, FL 34202
(913) 735-6488
ron@ameratech.com

Network Tools and Methods for Preventing Illegal Robocalls

Ameratech uses the following network tools to combat illegal robocalls:

(1) ANI Management Software. Using provider software, Ameratech identifies and blocks originating telephone numbers from sending calls believed to be unlawful based on repeat attempts to reach the network.

(2) Proactive Blocking. Ameratech blocks calls from phone numbers on Do-Not-Originate ("DNO") lists from its providers. In certain circumstances, Ameratech also blocks calls that originate from invalid, unallocated, or unused numbers. Ameratech's customers may also place certain inbound-only telephone numbers they use on the DNO list.

(3) Lawful Call Treatment. Ameratech applies no-block treatment to lawful robocalls so that they may complete. Call types include nonprofit, political calls, debt collections, surveys, school, healthcare, emergency notifications, and other lawful call types.

(4) Whitelist. Ameratech "whitelists" telephone numbers known to originate valid or legitimate calls.

(5) On-Going Customer Monitoring. Ameratech performs the following ongoing monitoring activities:

- Initial analysis of new customers' calling patterns to validate that they match their defined practices described in the KYC form;

- Utilization of various analysis tools to monitor traffic flow (ASR, ACD, ANI, DNIS, etc.) and generate alerts and optionally take actions based on configured thresholds and any suspicious activity;
- Ongoing monitoring of all calls to search for suspicious calling patterns; and
- When traffic analysis reports indicate potential suspicious calling, the appropriate responses are taken, which include some or all of the following: source traceback investigations; contacting the customer about suspicious activity; suspension of customers, traffic, or removal from the network until the customer can identify the source of suspicious activity; and collaboration with industry vendors and relevant enforcement agencies.

(6) Customer Contract Terms. Ameratech advises customers that they may be subject to random monitoring. All customers must agree to cooperate with traceback requests.

(7) Customer Relations. Ameratech provides ANI/Caller ID and blocking capabilities allowing customers to block calls from individual numbers or at the network level. Ameratech provides education and outreach to customers about robocall avoidance. Ameratech ensures no line-item charges for robocall mitigation appear on customer bills.

Additional STIR/SHAKEN Compliance Measures

In addition to implementing STIR/SHAKEN into networks as required, Ameratech actively engages with customers to achieve STIR/SHAKEN compliance by actively inquiring about their status.

Robocall Monitoring

Despite an extensive Know Your Customer vetting process, network management tools, proactive blocking, and collaboration with other carriers in the call stream, traceback activity and other analytics suggest that resourceful wrongdoers appear to find ways to pass through seams. Through fraud, deception, creative corporate maneuvering, and changing technology, robocallers continue to surface, negatively impacting contractual relationships and the industry as a whole.

Once Ameratech discovers suspicious calls or calling patterns, or suspects illegal robocalling or spoofing, Ameratech investigates to identify the party using the network to originate, route, or terminate the suspicious calls. Upon completing the investigation, Ameratech implements effective measures to eliminate the wrongdoer and reduce the wrongful activity if so determined.

Enforcement and Investigation History

As required by the Commission's expanded RMD filing requirements (47 C.F.R. § 64.6305(d)(2)(iv)), Ameratech discloses the following regarding its enforcement and investigation history:

- Ameratech has not been subject to enforcement action by the Commission.
- Ameratech has not been removed from, or prohibited from filing in, the Robocall Mitigation Database by Commission action.
- Ameratech has not been the subject of any Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- No law enforcement or Commission action bars Ameratech from the Robocall Mitigation Database.

In the event of any material change to the foregoing, Ameratech will update its RMD filing within ten (10) business days of such change, consistent with 47 C.F.R. § 64.6305.

Plan Updates

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. Ameratech will monitor industry best practices and continuously improve its internal processes to ensure this plan and its systems adapt to this ever-changing issue. In the event of any material change to this plan, Ameratech will make it available to employees, consultants, and contractors, and file such an update to the FCC Robocall Mitigation Database within ten (10) business days of such update, consistent with amended 47 C.F.R. § 64.6305(h).

AMERATECH CERTIFICATION

I, Ronald LaRoe, do hereby certify, under penalty of perjury, the following:

- a. Ameratech operates as an Intermediate Provider, neither terminating nor originating calls. Ameratech will only accept authenticated traffic that has been fully tokenized.
- b. Ameratech's business name and primary address are as follows:

Ameratech, LLC
11523 Palmbrush Trl, Ste 190
Lakewood Ranch, FL 34202
Phone: (913) 735-6488
President/CEO: Ronald LaRoe
Email: ron@ameratech.com
- c. Ameratech has no affiliates providing services regulated by the Commission. Ameratech has not operated as a foreign carrier.
- d. Ameratech has not been subject to FCC enforcement actions.
- e. Ameratech does not have, and has not previously used, any other business name.
- f. The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall mitigation-related issues follows:

Name: Ronald LaRoe
Title: President/CEO
Address: 11523 Palmbrush Trl, Ste 190
Lakewood Ranch, FL 34202
Phone: (913) 735-6488
Email: ron@ameratech.com
- g. Ameratech serves as an intermediate carrier in the call chain.
- h. Ameratech has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- i. Ameratech has not been the subject of a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- j. Ameratech OCN remains 472L.

Ronald LaRoe
President/CEO
Date: 2-26, 2026