

Robocall Mitigation Plan
Updated: February 27, 2026

EchoSpan Telecom Services LLC and its voice service affiliates¹ (collectively “EchoSpan Telecom”) submit this updated Robocall Mitigation Plan (“Plan”) as required by 47 CFR §64.6305(d). EchoSpan Telecom provides voice service to its customers and serves as a gateway provider for a limited portion of its total network traffic; the vast majority of EchoSpan Telecom’s call traffic originates and terminates domestically. EchoSpan Telecom no longer provides wholesale voice services and no longer serves as an intermediate provider in that capacity. This Plan applies to EchoSpan Telecom’s voice services and calling platforms across both (i) the Internet Protocol (“IP”) portions of its network and (ii) non-IP portions, including TDM-based segments that do not support SIP signaling.

1. STIR/SHAKEN Implementation & Non-IP Extension

EchoSpan Telecom has implemented the STIR/SHAKEN authentication framework on the IP portions of its network. Calls that EchoSpan Telecom originates on STIR/SHAKEN-enabled portions of its network are authenticated in accordance with applicable FCC rules, including 47 C.F.R. § 64.6301(a)(1)–(2). In addition to implementing STIR/SHAKEN, EchoSpan Telecom employs layered mitigation measures designed to reduce the origination and carriage of illegal robocall traffic, as further described below.

For portions of EchoSpan Telecom’s network that are non-IP and cannot originate, maintain, carry, process, and terminate SIP calls, EchoSpan Telecom relies on the continuing extension framework provided under 47 C.F.R. § 64.6304(d). Consistent with FCC rules and industry efforts, EchoSpan Telecom continues to evaluate non-IP mitigation and authentication solutions

¹ Identified in Appendix B.

through vendor relationships and relevant industry participation, including membership in USTelecom – the Broadband Association.

2. Robocall Mitigation Measures

EchoSpan Telecom maintains operational and contractual controls intended to prevent, identify, mitigate, and respond to suspected illegal robocall traffic. These measures include network analytics, blocking protocols, traceback participation, customer diligence, and escalation/termination practices.

2.1. Analytics and Monitoring

Using reasonable call analytics, EchoSpan Telecom uses an established process to identify suspicious calling patterns and to support investigation and mitigation (e.g., high volume, short duration, low completion rates). EchoSpan Telecom also participates in the registered industry traceback consortium and uses information learned through traceback participation to refine monitoring, analytics, and mitigation measures, as appropriate.

2.2. Blocking and Routing

Using reasonable analytics, EchoSpan Telecom maintains an established process for identifying and manually blocking calls originating on its network that are suspected to be spam, robocalls, or otherwise fraudulent, consistent with its role as a voice service provider and gateway provider. EchoSpan Telecom also participates in the registered industry traceback consortium and remains engaged at both the federal and state levels on robocall mitigation policymaking.

EchoSpan Telecom partners with Neustar to utilize a reputation-based solution to identify calls as likely spam for caller-ID-related services when the called party is a EchoSpan Telecom end user (business or consumer).

EchoSpan Telecom continues to monitor the development of additional call blocking and mitigation options, including options intended to provide customer controls and reduce false positives.

Certain permissive call-blocking approaches are not currently technically feasible for EchoSpan Telecom's network and are not available on a commercially reasonable basis in a manner that adequately mitigates the risk of large-scale inadvertent blocking of lawful calls. Nevertheless, EchoSpan Telecom actively monitors these developments and participates in relevant industry efforts.

EchoSpan Telecom is actively testing and monitoring the development of non-IP technology solutions for illegal and unwanted robocalls for potential future deployment.

3. 24 Hour Traceback Request Commitment

EchoSpan Telecom commits to responding fully and within 24 hours 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 that use its service to carry or process calls.

EchoSpan Telecom has not been the subject of any formal FCC, law enforcement, or regulatory agency action or investigation with findings of actual or suspected wrongdoing due to illegal robocalling or spoofing in the past two years.

4. "Know Your Customer" Reviews

EchoSpan Telecom conducts routine reviews of all new and renewed subscribers to confirm customer identity and support lawful use of EchoSpan Telecom's service. These reviews include collection and review of applicable business and contact information, which may include service address, billing address, point-of-contact details, nature of business, federal tax identification number, and other relevant information depending on customer type and services ordered.

EchoSpan Telecom requires completion of an application for service and may conduct credit checks in accordance with its customer contracting practices, this includes applying deposits or advanced payments when credit is not established. Where validation cannot be completed based on information provided, EchoSpan Telecom may request additional information before processing an application further.

EchoSpan Telecom also actively monitors its network traffic for patterns indicative of suspicious calling behavior and contacts customers proactively when such patterns are detected.

4.1. Employee Training

EchoSpan Telecom trains its sales teams to identify “red flags” that may indicate a prospective business customer could engage in fraudulent or illegal activity. These red flags include (but are not limited to):

- The prospective customer has little or no online presence;
- The prospective customer’s name includes certain terms (e.g., Telecom, Telecommunications, Tel, VoIP, Carrier, Call, Calling, Voice, Data, Com, Caller, LD, Long Distance, Internet);
- The prospective customer’s address is not the physical address of its business location (e.g., a UPS Store, a PO Box, or an address that is atypical for a business location, such as a data center or collocation facility, without a clear business justification);
- The prospective customer references least cost routing (“LCR”) capabilities, engines, or equipment;
- The prospective customer asks whether charges vary for rural areas;
- The prospective customer specifically requests a PRI, especially more than one;
- The prospective customer indicates it carries traffic other than for its own employees;
- The prospective customer provides calling diagrams or traffic-flow diagrams to discuss third-party traffic it wants EchoSpan Telecom to handle;
- The prospective customer is its own RespOrg; and/or • The prospective customer requests 4-digit precision calling.

Additionally, EchoSpan Telecom’s customer support team is trained to review indicators in prior bills that may suggest fraudulent or illegal activity. Specifically, these metrics include calls per second (“CPS”) relative to available concurrent calls (“CCs”) and average call duration. EchoSpan Telecom uses the following general guidelines:

- 1 CPS/100 CCs = Normal Traffic

- 2 CPS/100 CCs = Short Duration Traffic
- Minutes Of Use (MOU) Ratio for 1 CC = 15k Minutes
- Average call duration of 30 seconds or less

5. “Know Your Provider” Reviews

EchoSpan Telecom’s arrangements with upstream or interconnecting providers include contractual terms intended to support lawful use of service and ongoing operational coordination.

6. Contractual Terms In Place

EchoSpan Telecom’s voice service customers (including commercial business and residential customers) are subject to terms and conditions that prohibit unlawful use of service and preserve EchoSpan Telecom’s right to deny, suspend, or terminate service for violations of contract terms and/or applicable law.

These terms generally prohibit conduct that is unlawful, harmful to or interfering with EchoSpan Telecom’s network (or another provider’s network), interferes with other customers’ use or enjoyment of service, constitutes abuse (including spam-related abuse where applicable), creates a security risk, or violates privacy. The terms also prohibit transmitting material that intentionally or unintentionally violates applicable laws, rules, or regulations. EchoSpan Telecom has the right to terminate the service and contract if the customer does engage in such conduct with little to no advanced notice, based on the nature of the behavior. As a normal course of business operations, EchoSpan Telecom routinely reviews its contracts and makes necessary modifications to reflect the current state of regulations.