

Hammer Robocall Mitigation Plan

September 2, 2025

This Robocall Mitigation Plan (RMP) outlines the procedures and policies Hammer Technologies, Inc. (Hammer) has implemented to prevent the origination, carrying, or processing of illegal robocalls, consistent with the Federal Communications Commission's (FCC or Commission) existing robocall mitigation requirements.¹

I. Overview

Hammer, formerly known as Empirix, is a specialist provider of advanced quality assurance and active monitoring solutions for enterprise-scale voice networks and automated voice systems. Hammer offers customer experience (CX) assurance SaaS testing and active monitoring capabilities for large Fortune 1000 enterprises that want to ensure their customer-facing phone numbers are available, working properly, and with good voice quality. Specifically, Hammer's platform enables clients to create test scripts that simulate the end-customer calling into a self-service voice bot (IVR). Unlike traditional voice service providers, Hammer does not originate consumer-facing voice traffic over the public switched telephone network for general use. Instead, Hammer's platform functions as an artificial traffic generator that stimulates and analyzes call flows in controlled testing environments. Through this process, the enterprise client is able to validate expected system prompting and Dual-Tone Multi-Frequency (DTMF) or speech input responses, while also measuring the performance and quality of its voice system.

Hammer's network architecture is driven by the requirements of its enterprise clients to test their customer communications experiences. Our service model relies on partnerships with upstream telecommunications providers who supply call origination, transmission, termination, and telephone numbers, and who themselves comply fully with STIR/SHAKEN obligations or have implemented an appropriate robocall mitigation program. Accordingly, Hammer does not have control over the relevant network infrastructure to implement the technical requirements of STIR/SHAKEN and Hammer is not required under the Commission's existing rules to directly implement STIR/SHAKEN.²

Despite not being required to implement STIR/SHAKEN, Hammer is fully committed to adhering to the FCC's robocall mitigation directives, as applicable, and as further described below.

¹ See *Call Authentication Trust Anchor*, Sixth Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 17-97, FCC 23-18, at ¶¶ 29, 36-52 (Mar. 17, 2023); 47 C.F.R. § 64.6305(d).

² See *Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources*, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3260, ¶ 40 (2020). In addition, Hammer does not have an Operating Company Number (OCN) and is currently ineligible to receive a Service Provider Code token.

II. Robocall Mitigation Practices

Hammer has implemented the following reasonable steps to prevent the origination of illegal robocall traffic:

A. Know Your Customer (KYC) Procedures

- Conducting thorough pre-sales discovery and vetting of all potential customers and their use cases to ensure alignment with our testing solution capabilities. This includes verifying through electronic mail and live phone calls that the end customer works for a known, identifiable large enterprise business and can speak to their business and technical needs.
- Verification of customer reputation and credit worthiness through credit checks prior to order acceptance and service activation. Any questionable business will be vetted further to ensure they are reputable. Furthermore, self-activation is not allowed on the platform.
- Live onboarding training with customers to reinforce expected testing and monitoring usage of the platform. Inappropriate use will be promptly escalated to internal Hammer senior management and business leadership stakeholders and service will be suspended while investigation into the suspected activity occurs.
- Ongoing monitoring of customer traffic usage for quarterly business reviews hosted by Hammer customer success representatives.
- Immediate suspension or termination of service for customers found to be involved in illegal robocalls.

B. Know Your Upstream Provider

- Hammer contracts with U.S.-based third-party telecommunications carriers who originate, transmit, and terminate its calls. To the best of Hammer's knowledge, all of its third-party vendors are registered in the FCC's Robocall Mitigation Database and have complete STIR/SHAKEN deployments as well as robocall mitigation programs and policies.

C. Traffic Monitoring and Analytics

- Use of Infovista Ativa toolset to detect anomalous or unexpected call patterns. This is done from both a real-time and historical analytics standpoint.
- Ativa real-time monitoring also includes thresholds and alerting to proactively identify potential anomalies and allow for manual review of suspicious call activity.
- Audit logging is enabled within the SaaS testing application for all clients which tracks when users have created or manipulated a test script, making isolation of user activity much easier.

D. Call Authentication and Labeling

- Hammer uses caller ID validation techniques that identify Hammer calls as the originator “user agent” in the SIP header to uniquely identify Hammer Technologies as the source caller.

E. Complaint Handling and Remediation

- Dedicated support and operations teams to investigate platform complaints.
- Prompt response to consumer and regulatory complaints.
- Documentation of actions taken in response to complaints.
- 24x7 support available through email at support@hammer.com or website at <https://support.hammer.com/> to report complaints and remediate suspicious activity.

III. Traceback Requests

Hammer will cooperate with any FCC, law enforcement, or Industry Traceback Group (ITG) traceback requests and investigations; Hammer commits to respond within 24 hours to all traceback requests from such entities. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, Hammer employs a dedicated operations team and tooling able to search for and fetch call detail records and verify through call recordings the actual user journey flows to promptly complete and provide responses to all traceback requests received from the FCC, law enforcement and/or the ITG. Additionally, the Hammer team can uniquely identify the client, users, timestamps, and telco provider network the call was originated through.

IV. Compliance and Reporting

Hammer certifies that this mitigation plan is accurate and reflects our current policies and procedures.

Hammer will update its Robocall Mitigation Database filing within 10 business days of any material changes.