

STEVE SHEA INC

ROBOCALL MITIGATION PLAN UPDATED - FEBRUARY 2026

PURPOSE AND SCOPE

Steve Shea Inc (the “Provider”) is a voice service provider that originates voice traffic to the public switched telephone network (PSTN) and maintains a robocall mitigation program consistent with 47 CFR § 64.6305, including STIR/SHAKEN caller ID authentication implemented pursuant to 47 CFR § 64.6301(a).

PROVIDER ROLE / CALL FLOW

Steve Shea Inc provides hosted PBX/UCaaS services using 3CX systems deployed in Amazon Lightsail. Our customers are primarily retail and small-to-medium business clients who use our platform for inbound and outbound calling. All outbound SIP traffic is originated on our network by our end-user customers and delivered to our upstream carrier, Bandwidth, for PSTN termination. The Provider does not carry or transit third-party provider traffic; it only originates and manages traffic generated by its own customers, small-to-medium sized business clients, who use our platform for inbound and outbound calling. All outbound SIP traffic is originated on our network by our end-user customers and delivered to our upstream carrier, Bandwidth, for PSTN termination.

STIR/SHAKEN STATUS

Steve Shea Inc certifies that it has implemented STIR/SHAKEN caller ID authentication across the IP portions of its network for the SIP calls it originates, consistent with 47 CFR § 64.6301(a). The Provider’s network is IP-based for SIP calling, and the Provider authenticates caller identification information for originating SIP traffic.

The Provider signs outbound calls it originates using its own STI certificate issued by an approved STI Certificate Authority. The Provider uses third-party support for its STIR/SHAKEN implementation: Telonium serves as the STI-CA, issued the Provider’s signing certificate, and provides hosted signing for originating traffic (i.e., performs the technical signing function). While Telonium performs hosted signing, the Provider retains sole responsibility for attestation selection and compliance with the Commission’s STIR/SHAKEN rules and applicable technical standards. The Provider determines the attestation level based on its verification of the calling party and the calling party’s authority to use the associated telephone number(s). Calls are signed prior to downstream hand-off so terminating providers can verify the Identity header.

For inbound SIP calls received for termination/delivery to end users where caller identification information has been authenticated, the Provider verifies caller identification information where technically feasible and passes Identity headers downstream unchanged.

ROBOCALL MITIGATION MEASURES

a. KNOW YOUR CUSTOMER PROCEDURES

During onboarding, the Provider collects and verifies business identity information, including legal business name, physical address, primary contacts, and payment credentials. The Provider validates customers through public business records, contract execution, and payment verification, and confirms that the customer controls any telephone numbers they request to port. The Provider gathers expected use case and call volume information to help ensure traffic patterns align with normal business usage. Enhanced review is triggered by high-volume or short-duration traffic, marketing/dialer use cases, inconsistent caller ID behavior, or any

indicators of potential fraud or misuse.

Additionally, The Provider maintain Terms of Service and an Acceptable Use Policy that prohibit illegal robocalls, spoofing/unauthorized caller ID, misuse of numbering resources, and other unlawful or abusive calling activity. Customer agreements reserve the Provider's right to investigate, rate-limit, block, suspend, or terminate service for suspected or confirmed violations and to require supporting documentation when warranted.

b. TRAFFIC MONITORING, ANALYTICS, AND ENFORCEMENT

The Provider monitors call traffic using 3CX analytics, Bandwidth call event reporting, and internal alerting to detect anomalies such as sudden call bursts, abnormal ASR/ACD, short-duration spikes, or invalid caller ID patterns. The Provider also reviews Bandwidth's STIR/SHAKEN-related results and fraud alerts where available. When suspicious or potentially illegal traffic is detected, the Provider follows a defined escalation path: immediate review, customer notification, temporary blocking or rate-limiting, and suspension or termination if the issue persists or indicates malicious activity. The Provider maintains the right to disable outbound calling or specific caller IDs as needed to protect network integrity and comply with regulatory obligations.

c. KNOW YOUR UPSTREAM PROVIDERS

The Provider does not accept or transit third-party provider traffic; all traffic handled is generated by the Provider's own end-user customers on its hosted PBX platform. The Provider's upstream carrier for PSTN interconnection/termination is Bandwidth, with whom the Provider maintains a direct contractual relationship. The Provider maintains current escalation and traceback points of contact with Bandwidth, confirms the availability of call detail records needed to support investigations and traceback, and reviews upstream performance and fraud/robocall indicators on a periodic basis and upon suspected illegal traffic events.

TRACEBACK COOPERATION AND RESPONSE

The Provider has identified a single point of contact for traceback cooperation and remains committed to responding fully and within 24 hours to call traceback requests from the Commission, law enforcement, and the traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers initiating calls, including providing relevant call records and supporting information as requested.

PLAN GOVERNANCE

The Provider reviews and maintains its robocall mitigation program and updates it within 10 business days when filing information, services, traffic patterns, or risk controls change.