

RazorLine LLC Robocall Mitigation Plan

RazorLine LLC (“Razorline”) submits this Robocall Mitigation Plan (“Plan”) pursuant to 47 C.F.R. § 64.6305. This Plan describes Razorline’s efforts to mitigate illegal robocalls consistent with the FCC’s rules. Razorline may modify, add, delete, or otherwise alter any part of this Plan in order to respond to changes in its business, technologies, needs, industry best practices, or any applicable law or regulations. Razorline will update this Plan within ten (10) business days following the date of any changes to the Plan.

Razorline’s Roles in the Call Chain

Razorline operates as a voice service provider with a STIR/SHAKEN implementation obligation acting as a service provider originating calls and serving end-users.

STIR/SHAKEN Implementation Status

Razorline has implemented a STIR/SHAKEN call authentication solution provided by Bandwidth.com and Sinch, both recognized suppliers of carrier-grade voice network infrastructure. Their solutions enable the companies to authenticate outbound calls and verify inbound calls in accordance with FCC STIR/SHAKEN requirements and industry standards. STIR/SHAKEN functionality is integrated directly into Razorline’s production voice network using Ribbon SBCs and Skyvera and Microsoft Teams voice infrastructures. Authentication and verification are performed in real time as part of normal call processing, without requiring end-user action or modification to customer calling behavior. Razorline also leverages Ribbon’s Identity Hub services for inbound call screening.

This solution used by Razorline supports the full set of STIR/SHAKEN functional obligations, including:

- **Authentication and Attestation:**
Outbound calls are cryptographically signed by Bandwidth.com and Sinch, using Razorline-specific credentials and private key, and with attestation levels applied in accordance with Razorline’s relationship to the calling party and the associated telephone number resources.
- **Verification of Inbound Traffic:**
Inbound calls containing STIR/SHAKEN identity headers are validated to confirm the integrity of the signature and the originating provider’s attestation.
- **Standards and Governance Alignment:**
The solution is interoperable with industry certificate authorities and governance frameworks and conforms to applicable ATIS and SIP-based STIR/SHAKEN specifications.

Terms of Use/Acceptable Use Policies

Razorline maintains its terms of use and other conditions for the use of Razorline’s service that are intended to mitigate the ability for customers and end-users to originate robocall traffic on Razorline’s network.

Razorline's terms of service and acceptable use policies prohibit the use of Razorline's service in any manner that violates applicable law and reserves the right for Razorline to discontinue service to any customer in the event of such prohibited use. This includes Razorline monitoring usage patterns and terminating users in the event of prohibited uses such as robocalling.

New and Renewing Customer Vetting Process

Razorline maintains procedures that apply to the signing up of new and renewal of existing customers. Razorline maintains a direct contractual relationship with all its end-user customers. New and renewing customers are required to provide to Razorline, and maintain, accurate and complete information about themselves.

Upstream Provider Vetting Process

Razorline has policies and procedures in place to ensure it knows the identities of the new upstream providers from which Razorline accepts voice traffic. For example, before accepting traffic from new upstream providers, Razorline obtains information on an upstream provider's physical address, contact person, state or country of incorporation, federal tax ID (if applicable), the nature of their business, and whether the upstream provider is identified in the FCC's Robocall Mitigation Database. Razorline only accepts traffic from new upstream providers if they have a filing in the Robocall Mitigation Database and that filing has not been de-listed pursuant to an enforcement action. All traffic originating for individual customers come in and out the same upstream providers.

Authentication, Monitoring, and Mitigation

Razorline undertakes efforts to monitor the traffic that originates on or otherwise traverses its network. For example, Razorline investigates calling patterns that are indicative of caller ID spoofing or voluminous unwanted robocalling, including employing analytics and mitigation tools from third party providers, Nomorobo and Somos, to monitor Razorline's network for usual traffic patterns. Razorline prohibits use of its products or services in any way that is unlawful, harmful to or interferes with the use of Razorline's network or systems, or the network of any other provider, interferes with the use or enjoyment of services received by others, or constitutes abuse, among other prohibited uses. Razorline will take appropriate action which may include termination of service against customers and interconnection partners that fail to remedy practices that result in the transmission of significant volumes of unwanted robocalls.

In addition, by deploying Ribbon's Identity Hub solutions, Razorline has taken reasonable and effective steps to:

- Prevent the origination of spoofed calls using invalid or unauthorized numbers;
- Improve downstream carrier trust in authenticated traffic;
- Reduce the risk of call blocking or labeling of legitimate calls; and
- Comply with FCC expectations for active participation in industry-led robocall mitigation efforts.

Traceback Commitments

Razorline commits to respond fully, within 24 hours, to all traceback requests from the FCC, law enforcement and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers that use Razorline's service to originate, carry, or process illegal robocalls.