

Robocall Mitigation Plan

Arc Horizon LLC (DBA: Pathline)

Arc Horizon LLC (“Pathline”) submits this Robocall Mitigation Plan in compliance with **47 C.F.R. § 64.6305(d)(2)(ii)-(iii)** for inclusion in the FCC Robocall Mitigation Database.

Telnyx LLC (“Telnyx”) is an upstream provider of voice telecommunications infrastructure to Pathline.

Pathline provides cloud-based business communications functionality and relies on its upstream telecommunications provider, Telnyx LLC, for underlying voice connectivity and transmission facilities.

Pathline is a non-facilities-based interconnected VoIP provider that originates outbound voice traffic through its upstream carrier partner, Telnyx LLC. Pathline does not operate its own transmission facilities.

STIR/SHAKEN Implementation

Pathline routes all outbound voice traffic through its upstream provider, Telnyx LLC. Telnyx LLC implements STIR/SHAKEN authentication in accordance with FCC requirements.

Pathline does not operate its own STIR/SHAKEN authentication service or independently apply cryptographic identity headers to outbound calls.

- Pathline ensures that customers use telephone numbers that are assigned by Pathline or ported with authorization.
- Pathline does not permit customers to transmit unauthorized or unlawfully spoofed caller identification information.

Arc Horizon LLC (DBA: Pathline) provides interconnected VoIP functionality as part of its integrated business communications platform using underlying voice services provided by Telnyx LLC. Because Pathline does not own or control the network infrastructure required to independently deploy STIR/SHAKEN authentication, Pathline relies on its upstream provider for STIR/SHAKEN implementation. See 35 FCC Rcd. 3241 ¶ 40; 37 FCC Rcd. 6865 ¶ 36 & n.137; id. ¶ 45 & n.170.

Measures to Prevent Customers from Originating Illegal Calls and Know Your Customer (KYC) Procedures

Pathline permits its communications services to be used only for legitimate and lawful business purposes. Pathline’s user policy prohibits the use of its services for illegal robocalling, fraud, impersonation, harassment, deceptive practices, or any other unlawful or abusive activity.

During account creation, Pathline collects business and account information and requires valid payment credentials before or during service activation. Users must provide their full legal name, a valid email address, a valid phone number, and valid payment credentials, including name, card number, expiration date, CVC, billing address, and ZIP code. Payments are screened with Stripe Radar to aid in detecting potential fraud.

Pathline reviews customer account and payment information for indicators of fraud or abuse. Accounts presenting elevated fraud or abuse indicators may be subject to additional identity or business verification, including requests for additional personal information, such as government-issued identification.

Violation of Pathline's Terms of Service, Acceptable Use Policy, or applicable law may result in the immediate restriction, suspension, or termination of service.

Pathline prevents unauthorized caller ID use by limiting outbound calling to telephone numbers that the customer is authorized to use.

Voice Traffic Monitoring and Abuse Detection

Pathline monitors and reviews voice activity, including through manual review when appropriate, for indicators that may be associated with illegal robocalling, fraud, or abusive calling behavior. Relevant indicators may include unusual increases in outbound call volume, high call velocity, repeated short-duration calls, complaint patterns, anomalous geographic patterns, or traffic inconsistent with a customer's expected use case.

When suspicious activity is identified, Pathline may investigate the account and take proportionate mitigation action. Actions may include restricting outbound calling, temporarily suspending service, requesting additional verification, or permanently terminating the account.

Acceptable Use and Enforcement

Pathline's service policies prohibit customers from using the platform for illegal robocalling, unlawful telemarketing, fraudulent schemes, impersonation, unlawful caller ID spoofing, or calling practices that violate applicable federal or state law. Pathline's customers are responsible for obtaining any legally required consent and complying with applicable calling and telemarketing requirements.

Pathline reserves the right to investigate suspected violations and to restrict, suspend, or terminate service when necessary to protect users, upstream providers, telecommunications networks, or the public, or to comply with legal, regulatory, or carrier obligations.

Complaint Handling and Traceback Cooperation

Pathline cooperates in good faith with the Federal Communications Commission, law enforcement agencies, the Industry Traceback Group, upstream providers, and other authorized entities investigating suspected illegal robocall traffic.

Pathline will respond fully and within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement, and the Industry Traceback Group, and will cooperate with such entities in investigating and stopping illegal robocallers.

Where credible evidence indicates that a Pathline customer is responsible for illegal robocalling or related abuse, Pathline may restrict traffic, suspend or terminate the responsible account, preserve relevant records, and coordinate with its upstream provider or appropriate authorities.

Ongoing Evaluation

Pathline periodically evaluates its fraud prevention, customer verification, traffic monitoring, abuse response, and robocall mitigation practices. Pathline may update its controls in response to emerging abuse patterns, regulatory developments, upstream provider requirements, operational experience, and industry best practices.