

Pathway Communications
Robocall Mitigation
Program

Below is the Robocall Mitigation Plan filing for Pathway Communications. This plan will be submitted to the FCC's Robocall Mitigation Database and will be adapted to adjust to the latest laws, regulations, and industry best practices.

MITIGATION PROGRAM

As detailed below, Pathway has taken specific reasonable steps to avoid, the origination, carrying, or processing of illegal robocall traffic. All voice traffic that originates on our network is subject to the below Robocall Mitigation Plan.

Pathway monitors its network to identify suspicious traffic patterns, and has implemented anti-spoofing tools on its network to identify and block illegal calls and traffic. Based on information the Company receives from CDR and other carrier information, Pathway maintains an internal Do Not Originate ("DNO") list. Pathway periodically updates its tools and internal DNO list to detect and include invalid phone number formats, area codes, and unassigned number blocks. Pathway also utilizes internal data analytics to detect and investigate irregular and unexpected calling patterns, originating number use against customer profiles.

Pathway Communications has monitoring and reporting systems in place to analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls. Our monitoring systems provide alerts on calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated Telephone Number (TN) to detect patterns consistent with illegal robocalls.

If Pathway Communications detects a pattern consistent with illegal robocalls, or we have reason to suspect illegal robocalling or spoofing is taking place over our network, we will seek to identify the party that is using our network to originate, route, or terminate these calls. and take appropriate action.

Appropriate action may include:

- Validating that the originating party is authorized to use the TN.
- Suspending calling party's ability to originate, route, or terminate calls on Pathway Communications network.

Pathway's Know Your Customer requirements and processes include:

- Limiting a customer's capacity via call per second and/or concurrent session limits;
- Regularly checking call patterns for possible abusive traffic;
- Vetting all new customers and resellers with a combination of electronic and manual verification systems, credit reviews, references from trusted industry members, and previous experiences with customer executives and employees. Pathway severely limits the capabilities of new customers and resellers until these processes are complete.

Pathway examines the identity of its customers/resellers prior to entering into any contract to provide service. Pathway does not onboard customers/resellers if it is unable to verify the reseller's identification. This verification process includes confirmation of business names and addresses, EIN confirmation, confirmation of reseller in secretary of state databases and website verifications. Pathway's resellers are expected to verify their end-users consistent with federal and state robocall mitigation and anti-spoofing laws.

Pathway has an Upstream Provider. Pathway will confirm that its upstream providers are appropriately listed in the FCC's RMD and have not been delisted pursuant to an enforcement action.

Pathway works with its resellers to provide information concerning efforts to reduce illegal calls. Pathway's service agreements contain acceptable use and traffic integrity terms that prohibit the use of Company services for illegal purposes. Pursuant to our service agreements, Pathway may terminate services for fraudulent use of our services, for illegal, improper or unauthorized use of services, and/or for violations of any laws, rules and regulations applicable to the use of Company services. Pathway may block the originating number(s), terminating numbers(s), trunk(s) or customer, including termination of customer relationship to prevent robocalling, invalid originating number or spoofed origination number.

Pathway will respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping any robocallers that use our network to originate robocalls.

Traceback Cooperation

Pathway Communications commits to responding in a timely manner and supporting all traceback requests from the FCC, law enforcement, and the ITG.

Pathway reserves the right to modify and/or supplement this Robocall Mitigation Plan to adapt to risks and to improve the overall effectiveness of our program.

December 2025