

Company Name: Pinger, Inc.

FCC Registration Number (FRN): 0031337009

Operating Company Number (OCN): 348K

Primary Business Address:

Pinger, Inc.
2445 Augustine Drive
Suite 150
Santa Clara CA 95054

Robocall Mitigation Contact:

Larry Fleischer
VP, Customer Support
Customer Support
(408) 271-5711
larry@pinger.com
carrieradmin@pinger.com
legalcompliance@pinger.com

Introduction

Pinger, Inc. ("Pinger") is a voice service provider that has fully implemented the STIR/SHAKEN caller ID authentication framework across its IP network. This Robocall Mitigation Plan applies to voice calls originated using Pinger's voice service that are introduced into the U.S. telephone network. To the extent Pinger also offers non-interconnected VoIP services, those services are addressed only insofar as they relate to voice-call origination over the U.S. telephone network.

All calls originated on PINGER's network are signed and compliant with the Commission's STIR/SHAKEN standards. PINGER first certified its STIR/SHAKEN implementation in the FCC's Robocall Mitigation Database and has not had any prior certification removed or been prohibited from filing in the Database. This Robocall Mitigation Plan is submitted to describe the specific robocall mitigation practices that PINGER employs in compliance with FCC rules and orders. Pinger's robocall mitigation program includes the "reasonable steps" necessary to avoid originating illegal robocall traffic, with detailed practices reasonably expected to significantly reduce the origination of unlawful calls.

Pinger hereby certifies that all calls it originates are subject to this robocall mitigation program. In addition, Pinger confirms that it has never been, and is not currently, the subject of any formal FCC, law enforcement, or other regulatory action or investigation alleging illegal robocalling, spoofing, or a deficient mitigation program in the past two years. If Pinger or any affiliate had been subject to such an action, this plan would include a description of the investigation or

enforcement outcome, consistent with FCC requirements. Pinger understands that failure to maintain an effective robocall mitigation plan or to update its filing can result in removal from the Robocall Mitigation Database and other enforcement consequences. Pinger will complete any required annual recertification of its Robocall Mitigation Database filing, consistent with the Commission's rules, and will update required information within the required timeframe when changes occur.

Robocall Mitigation Program Commitments

Pinger has implemented a comprehensive robocall mitigation program tailored to its network and customers. In particular, Pinger makes the following core commitments, in line with the Commission's rules and the "reasonable steps" standard for robocall mitigation:

- **Reasonable Steps to Prevent Illegal Calls:** Pinger takes all affirmative, effective measures to prevent new or renewing users from using its network to originate illegal robocalls, in compliance with FCC regulations and orders. Pinger's program is designed to significantly reduce the origination of unlawful robocalls on its network, and Pinger diligently complies with the detailed practices outlined in this plan.
- **Rapid Traceback Response:** Pinger commits to respond fully and within 24 hours to all illegal robocall traceback requests from the FCC, law enforcement, and the industry traceback consortium. Pinger cooperates in good faith with these authorities and with the Industry Traceback Group to promptly investigate and halt any illegal robocall campaigns that may be transmitted through its services. This commitment to rapid traceback cooperation is a fundamental element of Pinger's mitigation program.
- **Industry Cooperation:** Pinger further pledges to cooperate with enforcement and industry efforts to combat unlawful calls. This includes collaborating with the FCC's Enforcement Bureau, federal and state law enforcement agencies, and other voice service providers to investigate and stop illegal robocallers using Pinger's network. Pinger actively participates in industry-led initiatives (such as the USTelecom Industry Traceback Group) and adheres to industry best practices for robocall mitigation and call authentication.

The following sections detail the specific reasonable steps and practices that make up Pinger's robocall mitigation program. These practices include robust customer identity vetting, advanced call analytics and blocking tools, and strict enforcement of anti-robocall policies.

Customer Vetting and Know-Your-Customer (KYC) Procedures

Pinger maintains strict know-your-customer (KYC) procedures to prevent bad actors from obtaining service and originating illegal traffic. In compliance with the FCC's requirement for affirmative measures on new and renewing customers, Pinger implements the following policies:

User Identity Verification: All users of our applications are exclusively available through the Apple's iTunes and Google Play stores providing unique advantages for verification of subscriber information. Specifically, in order to make use of either the Apple iTunes or Google Play stores, users must have established accounts with Apple and Google which requires the provision of a payment method, for users that make purchases, and an address associated with such payment method. Of course, Apple and Google maintain much more information on their users than simply

a payment method like device-related information, IP addresses used to connect to their stores and services, and many other data allowing for identifying individuals that make purchases or download apps including Pinger's app.

Pinger separately collects information from both free and paid users of its services to assess digital accounts, device-level information, IP addresses associated with users' accounts and in-app data. All of these data can also be used for verifying subscriber information and is accessible to law enforcement agencies when serving the company with the appropriate legal process to obtain such data.

Service Agreement and Usage Consent: Each user must agree to Pinger's Terms of Service and Acceptable Use Policy as a condition of service. These terms expressly prohibit using Pinger's network for any unlawful purpose, including initiating illegal robocalls, fraud, harassment, or spam calling of any kind. Users acknowledge that they may not use automated dialing equipment, spoof caller ID information in violation of law, or otherwise engage in abusive or fraudulent calling. Pinger's terms reserve the right to immediately suspend or terminate service for any customer that violates these prohibitions. Customers are clearly informed that all usage must comply with applicable laws and FCC rules, and that Pinger will monitor and enforce these requirements.

- **Ongoing Monitoring:** Pinger monitors users' accounts, especially new accounts, for signs of potential robocall abuse. Pinger's systems track calling patterns (call volumes, inbound-to-outbound ratio, account behavior, etc.) for abnormal activity and triggers alerts for further scrutiny. Pinger may deny, or restrict, new or high-risk account creation, or usage until a legitimate usage profile is established. These measures ensure that malicious actors are identified and stopped, fulfilling Pinger's duty to prevent new and renewing customers from originating illegal calls.

Through these KYC and customer vetting practices, Pinger meets its obligation to take effective steps to prevent customer-originated illegal calls. Pinger's customer vetting program was developed in line with FCC guidance and industry best practices, including the usage of third-party vendors to identify system level user attributes to keep bad actors out of its network from the start.

Upstream Provider Diligence and Traffic Sources

Pinger does not provide wholesale origination services and does not accept call traffic from upstream voice service providers for origination on Pinger's network. All outbound calls originated by Pinger originate from Pinger end-user accounts subject to the KYC and monitoring controls described above. If Pinger begins accepting traffic from upstream providers for origination or begins acting as an intermediate or gateway provider, Pinger will implement

upstream-provider due diligence procedures appropriate to that role and will update this plan and its RMD filing accordingly.

Network Traffic Monitoring and Analytics

Pinger employs advanced call analytics and network monitoring systems to identify and filter out illegal traffic. The FCC requires providers to describe any analytics systems used to identify or block illegal traffic (including third-party solutions), and Pinger has implemented a multi-layered analytics approach as part of its mitigation program:

- **Traffic Analysis:** Pinger's platforms continuously analyze call signaling and usage patterns across the network. The system is configured with algorithms to flag anomalies characteristic of illegal robocalls. For example, the analytics monitor metrics such as call volume, ratio of calls-to-texts, ratio of inbound-to-outbound calls and number of call recipients. When thresholds are exceeded or patterns match known fraudulent call rubrics, accounts may automatically be temporarily suspended or flagged for further review and potentially more significant intervention.
- **Machine Learning & Threat Intelligence:** Pinger leverages machine learning models and threat intelligence feeds to enhance detection of evolving illegal traffic. The machine learning models are trained on large datasets of user behavior to recognize subtle indicators of misuse. These tools enable Pinger's network to identify accounts that are likely acting unlawfully, even new or changing schemes, and adapt to them.
- **Third-Party Analytics Solutions:** In addition to in-house monitoring, Pinger utilizes third-party analytics vendors to augment illegal-activity detection and blocking capabilities. Pinger currently uses [REDACTED] to assess the risk of new account creations, and existing account logins, based on device and network attributes. Additionally, Pinger augments its intelligence through the utilization of monitoring alerts from ZipDX's RRAPTOR platform, which captures calls to RRAPTOR's honeypots. Pinger discontinues use of any listed vendor or adds a new vendor, Pinger will update its Robocall Mitigation Database information within the required timeframe.

Pinger continually refines its analytics and blocking techniques to adapt to new fraudulent tactics. Pinger's engineering and security teams regularly evaluate the performance of current tools and develop enhancements or new strategies as needed to stay ahead of evolving schemes. By combining automated monitoring, third-party data, STIR/SHAKEN authentication, and expert oversight, Pinger's analytics platform serves as an effective shield against illegal robocall traffic on its network.

Mitigation and Enforcement Actions

When Pinger's monitoring tools or external reports indicate that illegal robocall traffic is occurring on its network, Pinger takes swift and decisive mitigation actions to stop the offending traffic and prevent recurrence. These enforcement measures are a critical part of Pinger's program to actively police its network and deter bad actors. Pinger's mitigation and enforcement practices include:

- **Investigation of Alerts and Complaints:** Every internal alert of suspected illegal robocalls is promptly investigated by Pinger's fraud/security team. Additionally, Pinger promptly investigates any credible complaints or notifications it receives (from consumers, other carriers, regulators, etc.) regarding potentially unlawful calls on its network. Pinger uses call detail records, customer account data, and its analytics systems to trace the source of the suspicious traffic and determine the nature of the activity. No alert or complaint is ignored; each is treated as a serious potential violation.
- **Blocking of Illicit Traffic in Progress:** If a particular call campaign or call stream is identified as illegal, Pinger will immediately block that traffic on its network. Pinger can implement blocking at multiple levels – for example, blocking specific offending caller IDs or ranges, or disabling a particular customer's outgoing calls – depending on the scope of the incident. These network-level blocks are maintained as long as necessary to protect subscribers and the network. Pinger may also deploy temporary rules (such as blocking all calls to a particular area code or exchange that is being targeted by a scam) if warranted to stop ongoing abuses.
- **Customer Suspension and Termination:** If the source of illegal calls is determined to be one of Pinger's own customers, Pinger will immediately suspend that customer's service to halt any ongoing unlawful calls. Pinger will investigate whether the customer's account or equipment was compromised or if the activity was deliberate. Unless a clear innocent explanation is found and the customer ceases the offending activity, Pinger will move to terminate the customer's service for cause. Offending customers are promptly disconnected and blacklisted from returning to Pinger's network under known identities. This policy is clearly supported by Pinger's Terms of Service, which state that service may be terminated for any use of the service in violation of laws or FCC rules. By swiftly excising rogue customers, Pinger prevents repeat offenses and sends a strong message that illegal robocalling will result in loss of service.
- **Law Enforcement Referral:** Pinger complies with any formal cease-and-desist orders or other directives from government authorities concerning illegal robocall traffic. If Pinger uncovers evidence of a large-scale illegal robocall operation (for example, a fraud scheme targeting consumers), Pinger will preserve pertinent records and may proactively refer the matter to the FCC Enforcement Bureau or other appropriate law enforcement agencies.

Pinger will cooperate by providing information and support to help these authorities build cases against the bad actors. By facilitating enforcement beyond its own network, Pinger contributes to broader efforts to shut down robocallers and protect the public.

- **Post-Incident Analysis:** After any incident involving illegal traffic, Pinger conducts an internal review to strengthen its processes. The team analyzes how the illegal calls evaded any controls and identifies any gaps or areas for improvement in the mitigation program. Pinger then updates its practices or tools accordingly – for instance, adjusting analytics thresholds, adding new blocking rules, or revising customer vetting procedures – to reduce the likelihood of a similar incident. This continuous improvement loop ensures that Pinger learns from every event and adapts its defenses to be even more effective going forward.

By responding rapidly and effectively to any indication of illegal robocalling, Pinger ensures that such traffic is quickly eradicated from its network and that perpetrators face real consequences (loss of service and potential legal exposure). These mitigation and enforcement actions demonstrate Pinger’s commitment to actively police its network and fulfill the FCC’s expectation that providers will not knowingly or negligently allow illegal calls to persist on their systems. Pinger’s approach minimizes the duration and impact of any unlawful calling incident, protecting subscribers and the integrity of the wider telephone network.

Industry Coordination and Traceback Cooperation

Pinger fully recognizes that robocall mitigation is an industry-wide effort and actively coordinates with others in the telecom ecosystem to enhance the effectiveness of its program. Key cooperative measures in Pinger’s plan include:

- **24-Hour Traceback Response:** Pinger is firmly committed to responding within 24 hours to all traceback requests for suspected illegal calls. A dedicated representative at Pinger monitors traceback inquiries from the Industry Traceback Group (ITG) and the FCC’s traceback contacts. Upon receiving a traceback request, Pinger immediately investigates the call in question (using call logs to identify the source customer) and provides a complete and timely response with the requested information. Pinger recognizes that rapid response is critical to enabling the traceback process to quickly reach the origin of the call. This practice of prompt cooperation in tracebacks is not only required by FCC rules but is essential to the industry’s ability to identify and stop illegal robocalling operations in real time.
- **Cooperation with Investigations:** Pinger cooperates fully with any Commission or law enforcement investigations into illegal robocalling that involve its network or customers. If the FCC Enforcement Bureau or, for example, a state Attorney General’s office contacts

Pinger about suspect traffic, Pinger provides prompt and thorough assistance. This can include sharing relevant call records, customer account information (in accordance with privacy laws and legal process), and details of Pinger's own mitigation efforts related to the inquiry. Pinger will also comply with any specific requests, such as blocking certain traffic or preserving data, to aid an investigation does not impede or delay investigative efforts; instead, it views itself as a partner in the broader enforcement mission to shut down illegal activity.

- **Foreign Illegal Traffic Controls:** While Pinger's customer base is largely domestic, the company remains vigilant regarding international sources of illegal robocalls. If Pinger were to serve as a gateway for foreign-originated traffic, it would implement the additional safeguards required for gateway providers (such as verifying that foreign partners are not sending high volumes of illegal calls and blocking calls purporting to originate from numbers on the Do-Not-Originate list). Pinger stands ready to cooperate with the FCC's expectations for international call screening and will apply those measures if its business expands to include foreign traffic.
- **Robocall Mitigation Database Compliance:** Pinger will continue to maintain the accuracy of that filing. Pinger has designated a single company official as the point of contact for robocall mitigation issues and that contact's information is provided below:

Larry Fleischer

VP, Customer Support

Work: (408) 271-5711

Email:

Larry@pinger.com

Carrieradmin@pinger.com

Legalcompliance@pinger.com

Pinger will complete any required annual recertification of its Robocall Mitigation Database filing, consistent with the Commission's rules, including payment of any FCC filing fee that is applicable and effective at the time of submission and will update required information within the required timeframe when changes occur.

Pinger will update its Database filing within 10 business days if any of the information changes, such as a new contact person or a change in company ownership or name. Pinger will also submit any required annual re-certifications or additional information as the FCC's rules require, including the payment of the FCC's annual filing fee. In summary,

Pinger fully supports and adheres to the FCC's database requirements as a means of industry accountability.

Through these coordinated efforts, Pinger not only secures its own network but also contributes to the broader goal of protecting the U.S. telephone system and consumers from unlawful robocalls. Pinger understands that **no single provider can eliminate robocalls in isolation**, and thus it is engaged with regulators, law enforcement, and industry peers to collectively trace and **shut down illegal robocallers at the source**. Pinger's plan meets the FCC's expectations of cooperation and helps advance the Commission's top consumer protection priority of eliminating illegal robocalls.

Compliance Record and Ongoing Obligations

Pinger affirms that it has a clean compliance record regarding robocall mitigation. As stated above, neither Pinger nor any affiliated entity has been the subject of any formal FCC, law enforcement, or regulatory action or investigation for transmitting or facilitating illegal robocalls or spoofing, or for a deficient mitigation program, in the past two years. Pinger will maintain this high standard of compliance going forward.

Pinger acknowledges its ongoing duty to abide by current and future FCC robocall mitigation rules. This plan is designed to satisfy all applicable requirements of 47 C.F.R. § 64.6305 and the orders cited in the introduction (including the FCC's 2020 Call Authentication Second Report and Order establishing voice provider mitigation obligations, the 2021-2022 orders extending requirements to additional providers such as gateways, the Sixth Report and Order in 2023 expanding filing obligations, and the 2024-2025 actions to tighten filing compliance and impose penalties). Pinger will adapt its mitigation program and this plan as needed to remain compliant with any new rules or guidelines the FCC may issue. Pinger understands that the FCC and industry best practices may evolve, and Pinger will promptly implement any such changes to its procedures to ensure ongoing compliance and effectiveness.

By executing the practices detailed in this Robocall Mitigation Plan, Pinger strives to ensure that its network is inhospitable to illegal robocallers and that legitimate communications are safeguarded. This plan is suitable for submission to the FCC's Robocall Mitigation Database as evidence of Pinger's comprehensive mitigation program and compliance with all currently applicable FCC rules and orders. Pinger stands ready to assist the Commission in any further inquiries about this plan and will continue to collaborate with all stakeholders to eliminate illegal robocalls and restore trust in the nation's telecommunications networks.