



Plains Internet Robocall Mitigation Program Description

JOSEPH WARDLAW

Contents

1. Principals, Affiliates, Subsidiaries, and Parent Companies:	2
2. STIR/SHAKEN Implementation:	2
3. Customer and Provider Due Diligence:.....	2
4. Call Authentication Procedures:	3
5. Caller ID Verification Mechanisms:.....	3
6. Robocall Detection and Blocking Techniques:.....	3
7. Subscriber Tools and Controls:	3
8. Compliance with Regulatory Requirements:	4
9. Transparency and Reporting Mechanisms:	4
10. Industry Collaboration Efforts:	4
11. Continuous Improvement Strategies:.....	4

Plains Internet Robocall Mitigation Program Description 2026

1. Principals, Affiliates, Subsidiaries, and Parent Companies:

Principal(s): Plains Internet is led by Joseph Monroe, Chief Executive Officer (CEO), who oversees company operations and overall compliance with applicable FCC requirements, including robocall mitigation, caller ID authentication, and traceback cooperation. Andrew Monroe, Chief Operating Officer (COO), supports implementation of company policy, operational controls, and employee accountability related to these compliance obligations.

Affiliates/Subsidiaries/Parent Companies: Plains Internet operates as an independent entity and does not have any parent companies, subsidiaries, or affiliated entities relevant to this Robocall Mitigation Program description.

2. STIR/SHAKEN Implementation:

Plains Internet has implemented the STIR/SHAKEN caller ID authentication framework for outbound calling. Plains Internet has obtained its own Service Provider Code (SPC) token and STI certificate through the applicable authorized governance and certification authorities. Plains Internet utilizes Bandwidth's hosted signing service to apply STIR/SHAKEN signatures to outbound calls under Plains Internet's authority. Plains Internet applies Full (A) attestation to outbound calls when it knows the customer, has a direct relationship with the customer, and has verified the customer's right to use the calling number presented.

3. Customer and Provider Due Diligence:

Plains Internet follows a Know Your Customer (KYC) process for new customers, number assignments, and account changes. This process includes validating customer identity and business legitimacy, confirming authorized service contacts, and ensuring outbound caller ID is limited to numbers that are assigned to and authorized for use by the customer. Plains Internet does not permit customers to originate calls using arbitrary, misleading, or unassigned caller ID numbers.

4. Call Authentication Procedures:

Plains Internet applies call authentication controls to outbound traffic through its STIR/SHAKEN implementation and hosted signing arrangement with Bandwidth. For inbound and outbound call handling, Plains Internet uses its switching platform and related controls to evaluate call attributes and support mitigation measures intended to reduce the likelihood that unlawful robocall traffic or spoofed calling patterns traverse its network.

5. Caller ID Verification Mechanisms:

Plains Internet verifies caller ID use by restricting outbound caller ID presentation to telephone numbers that are assigned to, or otherwise specifically authorized for, the applicable customer. Outbound caller ID configuration is controlled by Plains Internet and/or authorized administrators. These controls are intended to prevent unauthorized caller ID substitution and to support accurate STIR/SHAKEN attestation.

6. Robocall Detection and Blocking Techniques:

Plains Internet enforces robocall mitigation and Do Not Originate (DNO) compliance through its switching platform, ioTran. ioTran performs automated checks against DNO and related datasets and blocks calls consistent with applicable FCC requirements, including calls associated with invalid numbers, unallocated numbers, inbound-only numbers, and numbers identified for DNO treatment. These controls are applied to both outbound call origination and inbound call processing, as appropriate. In addition, ioTran provides fraud and abuse mitigation controls designed to detect and reduce suspicious calling activity through pattern-based review, thresholds, and automated or manual actions such as blocking, throttling, service restrictions, and escalation for investigation. Plains Internet does not currently rely on third-party robocall analytics vendors for this function.

7. Subscriber Tools and Controls:

Plains Internet may provide customers with available service features that help them manage unwanted calls, including call handling and blocking-related features made available through the underlying platform or customer equipment where applicable. These tools supplement, but do not replace, Plains Internet's network-level robocall mitigation controls.

8. Compliance with Regulatory Requirements:

Plains Internet's Robocall Mitigation Program is designed to comply with applicable FCC rules and requirements, including the implementation of STIR/SHAKEN, reasonable steps to prevent the origination or transmission of illegal robocalls, compliance with applicable Do Not Originate blocking obligations, and cooperation with traceback requests. Plains Internet reviews its controls and practices as needed to remain aligned with current legal and operational requirements.

9. Transparency and Reporting Mechanisms:

Plains Internet maintains records and operational information sufficient to support internal review, traceback cooperation, and compliance oversight. Plains Internet commits to respond fully and within 24 hours to traceback requests from the FCC, law enforcement, and the industry traceback consortium. Plains Internet also maintains internal processes for reviewing suspicious activity and coordinating with upstream providers and other relevant parties when necessary.

10. Industry Collaboration Efforts:

Plains Internet coordinates with Bandwidth, ioTran, applicable industry partners, and regulatory authorities as needed to support lawful call authentication, traceback cooperation, and robocall mitigation efforts. This coordination supports consistent implementation of call authentication, DNO compliance, fraud mitigation controls, and prompt response to identified issues.

11. Continuous Improvement Strategies:

Plains Internet periodically reviews and updates its robocall mitigation controls to address evolving threats, changes in FCC requirements, and operational changes within its network. Material updates to call authentication, switching, blocking, fraud controls, or related compliance procedures will be reflected in internal documentation and, when required, in updated Robocall Mitigation Database filings.