

WebPerception Robocall Mitigation Program

1. Company Information

- **Company Name:** WebPerception, LLC
- **FRN:** 0036395507
- **Point of Contact:** Dan Jenkins, Director of Operations, info@webperception.com, 415.892.7711
- **Address:** 1701 Novato Blvd, Ste 103, Novato, CA 94947

2. Program Overview

WebPerception is committed to preventing the origination, transmission, and termination of illegal and unwanted robocalls across its network. As part of our obligations under 47 CFR § 64.6305, WebPerception implements a robust Robocall Mitigation Program (RMP) for all calls that are not authenticated under the STIR/SHAKEN framework.

3. Call Authentication (STIR/SHAKEN)

WebPerception has implemented STIR/SHAKEN for calls carried over IP where technically feasible. For non-IP portions of our network or where STIR/SHAKEN is not viable, the following mitigation efforts are in place.

4. Robocall Mitigation Measures

a. Know Your Customer (KYC)

WebPerception performs customer vetting at onboarding and continuously monitors usage to verify that customers are legitimate and authorized to originate calls. We:

- Require valid business documentation (e.g., EIN, articles of incorporation).
- Verify traffic patterns against declared use cases.
- Prohibit customers from using numbering resources not assigned to them or without authorization.

b. Traffic Monitoring and Call Analytics

WebPerception employs advanced call analytics and real-time monitoring to detect robocall patterns. We:

- Flag high-volume short-duration traffic and suspicious calling patterns.
- Maintain call logs and analyze anomalous behavior using automated tools and manual review.

- Immediately investigate and address flagged activity, including customer notification, throttling, or disconnection.

c. Traceback Cooperation

WebPerception fully cooperates with traceback requests from the Industry Traceback Group (ITG), the FCC, and law enforcement. We respond to all traceback requests within 24 hours and assist in identifying the source of illegal robocalls.

d. Call Blocking & Response Protocol

Upon identification of illegal or unwanted robocall activity:

- We notify the customer and request remediation or explanation.
- If unresolved, we suspend or terminate service in accordance with our AUP/TOS.
- We block known bad actors and numbers based on industry intelligence and internal blacklists.

5. Consumer Complaint Handling

WebPerception maintains an abuse reporting channel where consumers and other parties can report suspected robocall activity. Reports are reviewed within 48 hours, and appropriate action is taken.

6. Program Review and Updates

The Robocall Mitigation Program is reviewed quarterly and updated as needed to align with FCC guidance, industry best practices, and technological advancements.

7. Certification

WebPerception certifies the implementation and active operation of this Robocall Mitigation Program as required by the FCC's Robocall Mitigation Database.

Signed,

Dan Jenkins

Director of Operations

April 24, 2025