

Robocall Mitigation Plan

Parhelion Technologies Inc. Date of Submission: 09/16/2025

1. Introduction

This document serves as the Robocall Mitigation Plan (RMP) for Parhelion Technologies, in compliance with the Federal Communications Commission's (FCC) rules under the TRACED Act. The purpose of this plan is to detail the reasonable steps Parhelion Technologies takes to prevent the origination of illegal robocalls on its network and to cooperate with regulatory and law enforcement agencies in their efforts to combat unwanted and illegal calls.

Parhelion Technologies is committed to protecting its customers and the public switched telephone network (PSTN) from illegal robocall traffic. We recognize that effective mitigation requires a multi-faceted approach, including technical measures, customer vetting, and collaboration with industry partners.

2. VSP Information

- **Business Name(s):** Parhelion Technologies Inc.
- **Other Business Names in use:** N/A
- **Primary Business Address:** 5148 Saddle Ridge Road Plymouth Michigan 48197
- **FCC Registration Number (FRN):** 0035152933
- **Operating Company Number (OCN):** N/A
- **Point of Contact for Robocall Mitigation Issues:**
 - **Name:** Louis Donoghue
 - **Title/Department:** VP
 - **Email:** Louis@parhelion-tech.com
 - **Phone Number:** 734-453-7818 ext: 106

3. Robocall Mitigation Procedures

Parhelion Technologies employs the following reasonable steps and procedures to mitigate illegal robocall traffic:

3.1. STIR/SHAKEN Implementation

- **Implementation Status:** Parhelion Technologies has Fully implemented the STIR/SHAKEN framework on its IP-based network.
 - **Full Implementation:** For all calls originated on our IP-based network, we digitally sign the caller ID information with a full "A" attestation when we are the originating provider and we have a direct relationship with the customer.

3.2. "Know Your Customer" (KYC) Procedures

We have established and adhere to the following procedures to vet and monitor our customers to prevent the origination of illegal robocalls:

- **Customer Onboarding:**
 - We require all new customers to provide detailed business information, including legal name, physical address, and a designated point of contact.
 - We verify the customer's identity and business legitimacy, which may include checking public records, business registration databases, and online presence.
 - We conduct an initial review of the customer's intended use of our service to identify any potential red flags for high-volume or suspicious calling patterns.
- **Acceptable Use Policy (AUP):**
 - All customers are required to agree to and comply with our AUP, which explicitly prohibits the use of our services for illegal or fraudulent activities, including illegal robocalling, spoofing, and spamming.
 - The AUP specifies that providing false or misleading information to us is a violation of the terms of service.
- **Proactive Monitoring and Analytics:**
 - Our analytics system is configured to flag and alert us to anomalies such as:
 - Sudden, high-volume call spikes.
 - Calls with short durations (e.g., "short calls").
 - Large numbers of calls to numbers on Do-Not-Originate (DNO) lists.
 - Unusual calling patterns inconsistent with the customer's stated business purpose.
 - Repeated caller ID spoofing attempts.

3.3. Response and Remediation

- **Suspicious Activity Investigation:**
 - Upon detection of suspicious activity, we will initiate a prompt investigation. This includes reviewing call detail records (CDRs), contacting the customer, and requesting a legitimate use case for the flagged traffic.
 - If a customer is found to be originating illegal robocalls, we will take immediate action, which may include:
 - Issuing a warning.
 - Suspending the customer's account.

- Terminating the customer's service and blocking all associated phone numbers and accounts.
- We maintain a record of all investigations and actions taken.
- **Traceback Cooperation:**
 - Parhelion Technologies is committed to responding fully and within **24 hours** to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG).
 - Our designated point of contact and team are equipped to promptly access and provide the necessary information, including CDRs, to assist with traceback investigations.
 - We will cooperate with the ITG and other providers in the industry to collectively address and stop illegal robocalls.
- **Traffic Blocking:**
 - We will block traffic from any upstream provider that is not listed in the FCC's Robocall Mitigation Database.
 - We will block calls identified as highly likely to be illegal based on our analytics and traceback investigations.
 - We will also block calls from numbers on reasonable Do-Not-Originate (DNO) lists as provided by the ITG or other reliable sources.

4. "Know Your Upstream Provider" Procedures

Parhelion Technologies takes the following steps to ensure that its upstream providers are also committed to mitigating illegal robocalls:

- **RMD Verification:** We regularly verify that our upstream providers are listed and have a valid certification in the FCC's Robocall Mitigation Database.
- **Contractual Obligations:** Our contracts with upstream providers include provisions that require them to comply with all relevant robocall mitigation regulations and cooperate with traceback requests.
- **Due Diligence:** We conduct ongoing due diligence on our upstream providers to ensure they maintain effective robocall mitigation practices.

5. Plan Updates and Maintenance

This plan is a dynamic document that will be reviewed and updated regularly to reflect the evolving nature of illegal robocalling and new FCC requirements. We will update our filing in the Robocall Mitigation Database within ten (10) business days of any material change to this plan.

Louis Donoghue

[VP] [Parhelion Technologies]

