

Robocall Mitigation Plan

Annual Recertification - 2026

To comply with the Federal Communications Commission (FCC) regulations and ensure that our network does not originate illegal robocalls; while maintaining a high standard of service for our customers, Pathway Telco LLC strictly prohibits the use of our services for illegal robocalling activities, including but not limited to:

- Providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call.
- Violating any applicable local, state, or federal law.
- Using our services to engage in or in connection with fraudulent activities.

1. Know Your Customer (KYC)

We implement a robust KYC process to ensure that our customers are legitimate and do not engage in illegal robocalling activities. This includes:

- **Customer Verification:** Verify the identity of all customers to ensure they are legitimate businesses. The following items will be verified prior to onboarding:
 - Business location
 - FCC registration and FRN verification
 - Registered with USAC and 499a ID verification
 - Robocall Mitigation Plan has been filed in the Robocall Mitigation Database (RMD)
 - Customer is fully STIR/SHAKEN
- **Usage Monitoring:** Monitoring customer usage patterns to detect any suspicious activities, such as high call volumes to specific area codes or short-duration calls.
- **Action on Suspicious Activity:** Taking immediate action, including suspension or termination of service, if a customer is found to be engaging in illegal robocalling. This involves a detailed investigation and documentation of the findings.

2. STIR/SHAKEN Compliance

We are committed to implementing the STIR/SHAKEN framework across our network to authenticate caller ID information and prevent spoofed calls. This includes:

- All outbound calls must be authenticated using STIR/SHAKEN protocols.
- Users must ensure that calls are properly signed with the appropriate attestation level.
- Any detected spoofed or fraudulent calls must be reported immediately

3. Traceback

Pathway Telco LLC will commit to respond, within twenty-four (24) hours, to all traceback requests from the Commission, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating illegal robocallers that use its service to originate, carry, or process illegal robocalls. This includes:

- **Prompt Response:** Responding promptly to traceback requests, typically within 24 hours.
- **Information Sharing:** Providing all necessary information, such as call logs and customer details, to assist in the investigation of illegal robocalls.
- **Internal Documentation:** Maintaining detailed records of all traceback requests and our responses for future reference and compliance audits.

4. Compliance

We certify our compliance with the FCC's robocall mitigation requirements by filing our Robocall Mitigation Plan with the Robocall Mitigation Database. This includes:

- **Accurate Filing:** Ensuring that our filing is complete, accurate, and up-to-date, reflecting our current mitigation practices.
- **Timely Updates:** Updating our filing within 10 business days of any changes to our mitigation practices or company information.
- **Compliance Verification:** Regularly reviewing our filing to ensure ongoing compliance with FCC requirements.

5. Policy Review

We continuously review and improve our robocall mitigation practices to stay ahead of emerging threats and ensure compliance with regulatory requirements. This includes:

- **Policy Review:** Regularly reviewing our policies and procedures to identify areas for improvement.
- **Technology Upgrades:** Implementing new technologies and best practices to enhance our mitigation efforts, such as advanced call analytics and machine learning algorithms.
- **Staff Training:** Providing ongoing training for our staff to ensure they are knowledgeable about the latest robocall mitigation techniques and regulatory requirements.

6. Enforcement Actions

To ensure compliance with our robocall mitigation policies, we implement the following enforcement actions:

- **Warning Notices:** Issuing formal warning notices to customers found engaging in suspicious activities, outlining the specific violations and required corrective actions.
- **Service Suspension:** Temporarily suspending services for customers who fail to comply with our policies after receiving a warning notice. The suspension will remain in effect until the customer demonstrates compliance.
- **Service Termination:** Permanently terminating services for customers who engage in repeated or severe violations of our robocall mitigation policies. This includes providing written notice of termination and the reasons for the action.
- **Legal Action:** Pursuing legal action against customers who engage in illegal robocalling activities that cause significant harm to our network or reputation. This may include seeking damages and cooperation with law enforcement.

agencies.

- **Reporting Violations:** Reporting violations of our robocall mitigation policies to relevant regulatory authorities, such as the FCC, to ensure appropriate enforcement actions are taken.

7. Monitoring and verification

In accordance with the new FCC regulations regarding principals, affiliates, subsidiaries, and partner companies, we implement the following procedures:

- **Principal Verification:** Verifying the identity and legitimacy of principals, affiliates, subsidiaries, and partner companies through reliable and independent sources.
- **Affiliation Disclosure:** Requiring customers to disclose any affiliations with other companies, including principals, affiliates, subsidiaries, and partner companies.
- **Affiliation Monitoring:** Monitoring the activities of principals, affiliates, subsidiaries, and partner companies to ensure compliance with our robocall mitigation policies.
- **Affiliation Enforcement:** Taking enforcement actions against principals, affiliates, subsidiaries, and partner companies found to be engaging in illegal robocalling activities. This includes issuing warning notices, suspending or terminating services, and reporting violations to regulatory authorities.
- **Affiliation Reporting:** Reporting any affiliations with principals, affiliates, subsidiaries, and partner companies per FCC Robocall Mitigation Plan filing.

8. Do-Not-Originate (DNO) Compliance

Effective December 15, 2025, Pathway Telco LLC implements reasonable Do-Not-Originate (DNO) blocking consistent with FCC requirements.

Pathway Telco certifies that its DNO procedures are integrated into its broader robocall mitigation program, including STIR/SHAKEN implementation, KYC controls, and traceback cooperation under 47 CFR § 64.6305.

Pathway Telco maintains a DNO list that includes invalid, unallocated, and unused NANP numbers, inbound-only numbers, and other high-risk numbers identified through industry or government sources. The list is derived from reliable numbering data and internal fraud monitoring and is updated on a regular basis.

Network-level controls block calls that purport to originate from numbers on the DNO list.

Blocking applies to customer-originated traffic and calls transiting our network. Calls identified as using DNO numbers are automatically rejected prior to downstream transmission.

Traffic is continuously monitored for spoofing, invalid numbering patterns, and suspicious activity. Violations are investigated immediately and may result in suspension or termination.

Executed on February 25, 2026

Oliver Limonte

Managing Member

Pathway Telco LLC