

Nationwide Telecom Inc.

Robocall Mitigation Plan

Introduction

This Robocall Mitigation Plan outlines the comprehensive measures implemented by Nationwide Telecom Inc. to combat illegal robocalls and spoofing activities. The plan is designed to ensure compliance with the Federal Communications Commission (FCC) regulations, including the TRACED Act, 47 CFR § 64.6300 et seq., and other applicable laws and industry best practices. Nationwide Telecom Inc. is committed to protecting consumers from the harms of illegal robocalls by employing advanced monitoring, reporting, and mitigation strategies. This plan will be submitted to the FCC's Robocall Mitigation Database and will be regularly updated to address emerging threats and regulatory changes.

Key Objectives

1. **Prevent Illegal Robocalls:** Implement robust systems to detect, monitor, and mitigate illegal robocall activity originating from or transiting through our network.
2. **Ensure Compliance:** Adhere to all FCC regulations, including STIR/SHAKEN implementation, traceback requirements, and Know-Your-Customer (KYC) protocols.
3. **Protect Consumers:** Safeguard consumers from fraudulent, spoofed, and unwanted robocalls by proactively identifying and addressing suspicious activities.
4. **Collaborate with Stakeholders:** Work closely with regulatory bodies, law enforcement, and industry partners to investigate and mitigate illegal robocall operations.

Implementation of STIR/SHAKEN Framework

Nationwide Telecom Inc. has fully implemented the STIR/SHAKEN caller authentication framework across its IP-based network, as required under 47 CFR § 64.6302(b). All calls

originating from our network are authenticated to ensure the integrity of caller ID information and to prevent spoofing.

For non-IP portions of our network, Nationwide Telecom Inc. has adopted a Robocall Mitigation Program consistent with 47 CFR § 64.6305. This program includes alternative measures to authenticate caller identity and mitigate illegal robocalls, ensuring compliance with FCC requirements.

Monitoring and Detection Systems

Nationwide Telecom Inc. employs advanced monitoring systems to detect and analyze voice network traffic in real time. These systems are designed to identify patterns consistent with illegal robocall activity, including:

- **High-Volume Traffic Analysis:** Monitoring for unusual spikes in call volumes that may indicate robocalling campaigns.
- **Caller ID Validation:** Verifying the authenticity of calling numbers to detect invalid, unallocated, or spoofed numbers.
- **Reputation Monitoring:** Utilizing third-party services to flag numbers reported as spam or listed in the FCC consumer complaint database.

Real-time alerts are generated for any suspicious activity, enabling immediate investigation and mitigation.

Response to Suspicious Activity

In the event of detected suspicious activity, Nationwide Telecom Inc. will take the following steps:

1. **Traceback and Investigation:** Identify the source of the suspicious calls, including the originating, routing, or terminating party.
2. **Validation of Authorized Use:** Confirm whether the calling party is authorized to use the telephone number (TN) in question. Unauthorized or fraudulent use will result in immediate suspension or revocation of the TN.
3. **Suspension of Services:** Suspend the ability of the offending party to originate, route, or terminate calls through our network to prevent further illegal activity.

4. **Cooperation with Authorities:** Respond to traceback requests from the FCC, law enforcement, and the registered traceback consortium within 24 hours and provide full cooperation in investigations.

Subscriber and Provider Vetting Processes

Nationwide Telecom Inc. has established rigorous vetting processes to ensure the legitimacy of subscribers and upstream providers:

1. Subscriber Vetting:

- Residential, retail, and wholesale subscribers are vetted through standard business practices, including verification of service addresses.
- Outbound call centers and high-volume origination services undergo additional scrutiny, including stricter application reviews.
- Telephone numbers are validated to ensure subscribers only use numbers assigned or authorized to them.

2. Know-Your-Upstream Provider (KYUP):

- Nationwide Telecom Inc. maintains a comprehensive database of all carriers with which it exchanges traffic.
- Basic identification information, including physical business location, contact persons, and state of incorporation, is collected for all upstream providers.
- Interconnection agreements include clauses prohibiting illegal traffic and specifying traceback procedures.

Traceback and Reporting

Nationwide Telecom Inc. has designated a point of contact to handle traceback requests and incidents of illegal robocall traffic. This individual is responsible for:

- Responding to traceback requests from the FCC, law enforcement, and the registered traceback consortium within 24 hours.
- Cooperating fully in investigations to identify and stop illegal robocallers using our network.

Third-Party Partnerships and Tools

Nationwide Telecom Inc. leverages third-party solutions to enhance its robocall mitigation efforts:

- **Caller Authentication Services:** Utilizing tools such as TransNexus and Aureon's Caller Identification Authentication (CIDA) service to validate caller IDs and block high-risk numbers.
- **Outbound Shield Technology:** Preventing outbound calls from numbers reported as spam or identified as invalid.

Ongoing Compliance and Improvement

Nationwide Telecom Inc. is committed to maintaining compliance with all FCC regulations and industry standards. This plan will be reviewed and updated regularly to address new challenges, incorporate emerging technologies, and align with evolving regulatory requirements.

Certification

Nationwide Telecom Inc. certifies that:

1. It has implemented a Robocall Mitigation Program consistent with 47 CFR § 64.6305.
 2. It has not been the subject of any formal Commission, law enforcement, or regulatory action related to illegal robocalls or spoofing.
 3. All required information, including the designated point of contact, has been submitted to the FCC's Robocall Mitigation Database.
-