

Robocall Mitigation Plan

1. Introduction

This document outlines the Robocall Mitigation Plan for Skycreek Corporation, a voice service provider specializing in outbound automated calls for customer care purposes such as account notifications, appointment reminders, and follow-up surveys. Our operations prioritize compliance with the Federal Communications Commission (FCC) regulations, particularly **47 CFR § 64.6301(a)(1)(2)**, and industry best practices to mitigate illegal robocalls.

2. Company Information

- **Company Name:** Skycreek Corporation
 - **FCC Registration Number (FRN):** 0031362312
 - **Contact Information:** Mark Wilburn, mark_wilburn@skycreek.com, 703-402-0962
-

3. Robocall Mitigation Strategies

3.1 Customer Vetting and Call Flow Approval

- All customers must sign a **Master Service Agreement** for engagement with Skycreek and **Statement of Work (SOW)** with campaign details outlining the nature and purpose of their calls.
- Each customer's call flow, scripts, and use cases are reviewed for compliance before production deployment.
- Customers are prohibited from transmitting illegal or unethical robocalls, and service agreements explicitly enforce compliance.

3.2 Caller ID Management

- Require customers to provide verified and legitimate caller IDs, such as contact center or office callback numbers.
- Ensure that all caller IDs are validated before use and monitor their compliance with FCC rules and STIR/SHAKEN standards.

3.3 Call Authentication

- **Bandwidth Integration:**
Calls initiated using Bandwidth's SDK comply with the **STIR/SHAKEN framework**. Bandwidth authenticates and verifies caller IDs with appropriate **SHAKEN attestation levels**.
- **Legacy System on Level 3:**
A limited number of calls are routed through a legacy system on Level 3, which does not fully support STIR/SHAKEN. Interim mitigation measures include:
 - Manual caller ID validation and monitoring for traffic anomalies.
 - A phased migration plan to transition all calls to Bandwidth by 03/31/2025

3.4 Monitoring and Collaboration

- **Call Pattern Monitoring:**
Deployed analytic tools to monitor call patterns, detect irregularities, and identify potential misuse.
- **Threshold Alerts:**
Set thresholds for abnormal traffic, such as unexpected volume spikes or anomalous call durations, and flag suspicious activities for review.
- **Collaboration with Providers:**
 - Work with Bandwidth to ensure compliance with STIR/SHAKEN and address flagged traffic.
 - Coordinate with Level 3 during the transition to monitor call traffic and prevent illegal robocalls.
- **Complaint Resolution:**
Investigate complaints promptly, taking corrective measures such as account suspension or enhanced caller ID validation.

3.5 Data Security and Integration Practices

- **Secure Data Transmission:**
 - All data files are transmitted via **Secure File Transfer Protocol (SFTP)**.
 - Our customers use secure APIs available over VPN for submitting data for calls through Bandwidth and Level 3 systems.
- **System Integration:**
Integration with customers' billing and workforce management systems occurs exclusively over **VPN connections** to ensure data security.
- **Access Control:**
Restrict data access to authorized personnel and conduct regular audits.

3.6 Information Security Certification

- Skycreek Corporation is **ISO 27001:2022 certified**, reflecting our commitment to global standards for information security.
- Certification ensures robust security practices, including risk mitigation, access control, and structured incident response.

3.7 Compliance with 47 CFR § 64.6301(a)(1)(2)

- Implement a Robocall Mitigation Program to ensure all calls are legitimate and authorized by customers.
- Participate in the **STIR/SHAKEN framework** through Bandwidth and implement alternative measures for non-IP traffic on the Level 3 system during its transition phase.
- Register robocall mitigation practices in the FCC's **Robocall Mitigation Database** and provide updates as necessary.

3.8 Traceback Cooperation and Rapid Response

- **Traceback Participation:**
Fully cooperate with the Commission, law enforcement, and the registered traceback consortium to identify and mitigate illegal robocall activity. Provide call records and relevant information promptly for traceback investigations.
- **24-Hour Compliance Commitment:**
 - Respond to any traceback or regulatory inquiry within **24 hours**.

- Take immediate corrective actions, such as blocking flagged traffic or notifying customers of non-compliance.
-

4. Call Purposes and Legitimate Use Cases

Skycreek Corporation supports only legitimate and authorized use cases, including:

- **Account Notifications:** Updates regarding account status, payment reminders, or important alerts.
 - **Appointment Reminders:** Notifications of upcoming appointments or schedule changes.
 - **Follow-Up Surveys:** Post-service feedback requests or customer satisfaction surveys.
-

5. Review and Updates

This Robocall Mitigation Plan is reviewed and updated annually, or as required, to reflect:

- Changes in regulatory requirements or industry standards.
 - Updates to systems and technologies.
 - Improvements in business practices and customer needs.
-

6. Certification

I, Mark Wilburn, COO, hereby certify that Skycreek Corporation has implemented the measures outlined in this Robocall Mitigation Plan and is committed to compliance with the FCC's robocall mitigation requirements.

Signature:

Mark Wilburn, COO

01/01/2025