



Robocall Mitigation Plan

This document describes the comprehensive robocall mitigation program implemented by X2nSat, Inc., addressing the requirements outlined in 47 CFR § 64.6305(d)(2)(ii), (e)(2)(ii), and (f)(2)(ii). Our program leverages our existing infrastructure to actively prevent, identify, and block illegal robocall traffic.

X2nSat Service Overview

X2nSat is a small voice services reseller with fewer than 100,000 subscriber lines offering Business Continuity (failover) voice services to the customers in the Healthcare and Public Utility industries. All services use private IP networks over the satellite making it easier to traceback an illegal robocall.

1. Specific Reasonable Steps to Avoid Originating, Carrying, or Processing Illegal Robocall Traffic over the X2nSat Private Satellite Networks

Our robocall mitigation program employs a multi-faceted approach to prevent the origination, carrying, and processing of illegal robocall traffic. Key steps include:

- **Traffic Monitoring and Analysis:** We continuously monitor call traffic patterns for anomalous behavior indicative of illegal robocalling. This includes analyzing call volume, call duration.
- **Managed IP Handsets:**
 - The IP handsets are configured with robust security settings, including strong password policies and are only accessible over the private networks.
 - We utilize PBX's internal logging and reporting to identify unusual activity originating from IP handsets, such as excessive failed registrations or unusually high outbound call volumes from individual extensions.
- **Number Management:** We regularly review and manage our assigned telephone numbers, taking steps to identify and remove unused or cancelled numbers.
- **Internal Policies and Training:** Our staff receives regular training on identifying and responding to potential illegal robocall attempts and understanding their role in maintaining the integrity of our private network.



2. Compliance with Obligation to Know Our Customers and/or Upstream Providers

Our commitment to knowing our customers and upstream providers is fundamental to our robocall mitigation efforts:

- **Customer Onboarding and Vetting:**
 - For new customers, we conduct a thorough vetting process that includes verifying business registration, contact information, and intended use of our services.
 - We require all customers to agree to terms of service that explicitly prohibit abusive practices.
 - Ongoing monitoring of customer traffic patterns helps us identify deviations from their typical usage profiles that might indicate unauthorized or illegal activity.
- **Upstream Provider Due Diligence:**
 - We engage only with reputable upstream SIP trunk providers who demonstrate a commitment to robocall mitigation and compliance with industry standards.
 - We maintain clear communication channels and agreements with our upstream providers regarding traffic types, acceptable use, and procedures for addressing suspicious activity.
 - Regular reviews of our upstream provider relationships are conducted to ensure ongoing compliance and performance in combating illegal robocalls.

3. Analytics System(s) Used to Identify and Block Illegal Traffic over the X2nSat Private Satellite Networks

Our primary analytics system for identifying and blocking illegal traffic is built around our **Session Border Controller**.

- **Real-time Traffic Analysis:** The SBC provides real-time visibility into SIP and RTP traffic, allowing us to analyze call metadata, call setup patterns, and media streams. It monitors for:
 - **High Call Volumes/Short Durations:** Rapid detection of calls with high volume and very short durations.
 - **Unusual Call Patterns:** Identification of unusual outbound call patterns from specific IP ranges, originating numbers, or destination numbers.
 - **Anti Spoofing Detection:** While STIR/SHAKEN provides robust attestation, the ProSBC can identify suspicious or malformed Caller ID information.
- **Automated Blocking Rules:** Based on the analytics and observed patterns, the SBC is configured with rules to:
 - **Block Calls:** Immediately block calls identified with invalid calling numbers.
 - **Rate Limit:** Apply rate limits to specific calling parties or destinations exhibiting excessive or anomalous call volumes.
- **Logging and Reporting:** The SBC generates extensive logs of all call attempts, security events, and policy actions. These logs are used for:
 - **Post-Mortem Analysis:** Investigating identified illegal traffic to understand its characteristics and improve future mitigation strategies.



- **Compliance Reporting:** Generating reports necessary for regulatory compliance and internal audits.

4. Third-Party Analytics Vendor(s)

Currently, X2nSat, Inc. does not utilize any dedicated third-party analytics vendors specifically for robocall identification and blocking. Our robocall mitigation program relies primarily on the native analytics and security capabilities of our SBC, combined with internal monitoring and policy enforcement.

Should our needs evolve, we would consider reputable third-party solutions that integrate effectively with our existing infrastructure and further enhance our ability to combat illegal robocall traffic.