

# FCC Know Your Customer (KYC) and Robocall Mitigation Policy

**Policy Version:** 1.3

**Effective Date:** September 26, 2025

## 1. Purpose

The purpose of this policy is to establish and document the procedures for our Know Your Customer (KYC) and robocall mitigation program. This policy is designed to ensure compliance with all applicable FCC regulations, including the requirement for voice service providers to take affirmative, effective measures to prevent the origination of illegal robocalls on their networks.

## 2. Scope

This policy applies to all telecommunication services provided by ProStratus LLC and to all personnel involved in customer management, sales, and network operations.

## 3. Customer Identification Program (CIP)

Because our business model is based on established, long-term relationships with clients, our CIP focuses on documenting and regularly verifying existing customer information.

### 3.1. Customer Records

For each client, we maintain a comprehensive file containing, at a minimum, the following information:

- **Business Profile:** Full legal name of the business, primary business address, and nature of the business operations.
- **Beneficial Ownership:** Identification of all ultimate beneficial owners (UBOs) holding a 25% or greater interest in the business, along with their names, titles, and contact information.
- **Key Contacts:** Names, titles, and contact details for the primary individuals responsible for managing the account.
- **Relationship History:** Detailed records of the business relationship, including the start date and any significant service history.

### 3.2. Ongoing Verification and Refresh

Customer identity verification is not a one-time process. Our policy includes perpetual KYC (pKYC), which involves regular verification and refreshing of customer data.

- **Annual Review:** All customer records are reviewed and updated annually. This includes:
  - Confirming the accuracy of all customers and UBO information.
  - Verifying that contact information for key personnel is current.
  - Conduct enhanced due diligence (EDD) for any customer whose risk profile may have changed.
- **Trigger-Based Review:** A review is triggered and completed within 30 days of any of the following events:
  - Change in ownership structure.
  - Notification of a change in business operations or address.
  - Identification of unusual activity during our continuous monitoring process.

## 4. Ongoing Monitoring and Risk Management

Our proactive approach to monitoring is a core component of our robocall mitigation strategy. It allows us to detect and respond to suspicious activity before it can result in regulatory violations.

### 4.1. Real-Time Traffic Analysis

We employ real-time usage monitoring to identify anomalous calling patterns that may indicate illegal activity. Our monitoring system tracks:

- **Call Volume and Rate:** Unusual spikes in call volume or calls per second (CPS) for a given client are automatically flagged for review.
- **Call Duration:** Short-duration or "one-ring" calls are monitored, as they are a hallmark of illegal robocalling campaigns.
- **A-Level Attestation:** Our system tracks and verifies that calls originating from our network are assigned the appropriate A-level STIR/SHAKEN attestation, which

signifies that we have authenticated the subscriber and confirmed their authorization to use the calling number.

- **Customer-Specific Patterns:** Our familiarity with client-specific usage patterns allows us to quickly identify any deviation from normal behavior.

#### 4.2. Incident Response and Mitigation

Upon identification of unusual or potentially illegal call patterns, the following actions are immediately taken:

- **Automatic Blocking:** The network is configured to automatically block traffic from customers when their activity exceeds pre-defined, risk-based thresholds.
- **Immediate Investigation:** The designated compliance officer is immediately notified to initiate a manual investigation.
- **Client Contact:** The compliance officer contacts the client to discuss the flagged activity and determine the cause.
- **Corrective Action:** Based on the investigation, [Your Company Name] will take corrective action, which may include:
  - Requiring the client to provide a legitimate business reason for the traffic.
  - Implementing stricter rate limits or other controls.
  - In cases of suspected illegal activity, immediately terminating the client's service.
- **Enforcement Reporting:** We maintain a process to cooperate fully with FCC robocall investigators and report suspicious activity when required.

### 5. Policies and Procedures

#### 5.1. No "Established Business Relationship" Exemption

We acknowledge and operate under the understanding that an "established business relationship" is no longer a valid exemption for telemarketing calls and does not mitigate the need for robust KYC procedures.

## 5.2. Policy Revisions

This policy is reviewed and updated at least annually to reflect changes in our business practices, technology, and FCC regulations.

## 6. Recordkeeping

We maintain accurate and easily retrievable records of all KYC activities for a minimum of one year. These records include:

- Original and updated customer identification information.
- Documentation of all ongoing monitoring activities.
- Records of all suspicious activity alerts and the subsequent investigation and resolution.
- Training records for all personnel involved in customer and compliance matters.

## 7. Training

All employees involved in customer-facing roles, network operations, and compliance receive regular training on this policy and FCC robocall mitigation requirements.

Training includes how to identify red flags and escalate suspicious activity.

## 8. Responsibility

The **Compliance Officer** is responsible for overseeing the implementation and enforcement of this policy. All employees are responsible for adhering to its guidelines.

## 9. Certification Statement

I certify that the information provided in this robocall mitigation program description is true and accurate to the best of my knowledge, and that we are actively engaged in preventing unlawful robocall traffic.

Signature:



Name and Title: Craig S Terrell - CIO

Date: 09/30/2025