

## Robocall Mitigation Program Description

**Company Name:** Sylvia Systems

**FRN:** 0031380678

**Underlying Carrier(s):** VOIP.MS

**Date:** 2/13/2026

---

### 1. Company Classification

Sylvia Systems is a **non-facilities-based interconnected VoIP reseller**. We do not own or operate transmission facilities and rely on one or more underlying domestic carriers for origination and termination of voice traffic.

This Robocall Mitigation Program is established in accordance with the rules and orders of the Federal Communications Commission (FCC), including the TRACED Act and applicable FCC robocall mitigation requirements.

---

### 2. Network Architecture & Traffic Flow

- We provide VoIP services to end users and/or business customers.
- All outbound PSTN traffic is transmitted through our contracted underlying carrier(s).
- We do not directly interconnect with the PSTN.
- We do not assign numbering resources independently unless specifically authorized.

Our mitigation program operates at the **customer onboarding, service level, and traffic monitoring levels**, while we coordinate with our underlying carrier(s) for network-level blocking and authentication.

---

### 3. STIR/SHAKEN Status

As a non-facilities-based VoIP reseller:

- We rely on our underlying carrier(s) to implement STIR/SHAKEN authentication on outbound traffic.
- We coordinate with underlying providers to ensure proper attestation levels.

- We provide accurate customer and call origination information necessary to support appropriate attestation.
- We do not manipulate caller ID information in a manner inconsistent with FCC rules.

If we control numbering resources, we ensure numbers are properly associated with authorized customers before use.

---

## **4. Know Your Customer (KYC) & Due Diligence**

We implement strict onboarding procedures prior to activating any voice services.

### **4.1 Customer Verification**

We collect and verify:

- Legal business name
- Articles of incorporation or business registration
- EIN verification
- Physical address (no PO boxes without additional verification)
- Government-issued identification (when applicable)
- Beneficial ownership information
- Nature of business and calling purpose

### **4.2 High-Risk Use Case Screening**

Enhanced due diligence is conducted for:

- Telemarketing
- Lead generation
- Debt collection
- Political calling
- Healthcare marketing
- Insurance or financial services

We may require:

- Sample call scripts

- Proof of consent procedures (TCPA compliance)
  - Website and online presence verification
  - Third-party compliance documentation
- 

## **5. Traffic Monitoring & Analytics**

Although we do not control underlying switching infrastructure, we actively monitor traffic patterns through:

### **5.1 Call Detail Record (CDR) Review**

- Daily CDR monitoring
- ASR (Answer-Seizure Ratio) analysis
- ACD (Average Call Duration) tracking
- Short-duration call detection
- High-volume anomaly detection

### **5.2 Automated Alerts**

We flag:

- Sudden traffic spikes
- Neighbor spoofing patterns
- Sequential dialing behavior
- High complaint correlation

### **5.3 Coordination with Underlying Carrier**

When suspicious traffic is detected:

- We notify the underlying carrier immediately
  - We cooperate with blocking requests
  - We suspend or restrict customer traffic pending investigation
- 

## **6. Caller ID & Numbering Controls**

We prohibit:

- Unauthorized caller ID spoofing
- Use of invalid, unallocated, or unassigned numbers
- Use of numbers without documented customer authorization

Customers must certify that:

- They have the right to use all numbers presented as caller ID
  - They comply with the Telephone Consumer Protection Act (TCPA)
  - They do not engage in unlawful robocalling
- 

## **7. Complaint Handling & Traceback Response**

### **7.1 Complaint Intake**

Complaints may be received from:

- Consumers
- Upstream carriers
- Industry traceback groups
- Regulatory agencies

### **7.2 Investigation Process**

1. Immediate logging of complaint
2. CDR review and call trace
3. Identification of originating customer
4. Customer notification and demand for explanation
5. Determination of corrective action

### **7.3 Traceback Cooperation**

We fully cooperate with traceback requests, including those coordinated by the U.S. Telecom Industry Traceback Group.

We:

- Respond within required timelines
  - Provide accurate customer identification
  - Maintain CDRs for a minimum of 12 months
  - Take mitigation action when unlawful traffic is identified
- 

## **8. Enforcement Actions**

If a customer is suspected of illegal robocalling activity, we may:

- Issue a formal warning
- Require written compliance attestation
- Implement traffic caps
- Block specific DIDs
- Suspend outbound calling privileges
- Immediately terminate service
- Report activity to our underlying carrier(s)
- Report activity to appropriate authorities when warranted

We maintain a zero-tolerance policy for knowingly illegal robocalls.

---

## **9. Record Retention**

We retain:

- Customer onboarding documentation
- Identity verification materials
- CDRs (minimum 12 months)
- Complaint logs
- Investigation reports
- Enforcement documentation

All records are securely stored and available upon lawful request.

---

## 10. Employee Oversight & Compliance Governance

- A designated Compliance Officer oversees this Robocall Mitigation Program.
  - Employees with access to voice provisioning or customer onboarding receive compliance training.
  - We conduct periodic internal reviews of mitigation effectiveness.
  - We review FCC updates and industry guidance to ensure continued compliance.
- 

## 11. Mitigation Strategy Certification

As a non-facilities-based VoIP reseller, we mitigate robocall risk through:

- Strict customer vetting
  - Ongoing traffic monitoring
  - Rapid complaint response
  - Cooperation with traceback efforts
  - Coordination with underlying carriers for network-level mitigation
  - Immediate enforcement against non-compliant customers
- 

### Certification

I certify under penalty of perjury that:

1. Sylvia Systems has implemented the robocall mitigation practices described herein.
2. The information provided is true and correct to the best of my knowledge.
3. We will comply with all applicable FCC robocall mitigation requirements.

### Authorized Representative:

Name: John Sylvia

Title: CEO

Signature: John Sylvia

Date: 2/13/2026

