



InfiCloud STIR/SHAKEN Caller ID Authentication and Robocall Mitigation Program

Formal FCC Compliance Submission

Pursuant to 47 CFR § 64.6305

Service Provider: Infimobile (MVNO)

Underlying Network Operator: Verizon Wireless

Submission Date: February 26, 2026

Document Classification: Regulatory Compliance Submission

Version Control and Revision History

Version	Date	Author	Description
1.0	Feb 26, 2026	InfiCloud Compliance Division	Initial FCC submission

Table of Contents

- 1 Regulatory Compliance Statement
- 2 STIR/SHAKEN Framework Implementation
- 3 Robocall Mitigation Program Overview
- 4 Traffic Monitoring and Enforcement Controls
- 5 Traceback Cooperation and Contact Information
- 6 Certification Statement
- 7 Appendix A – Compliance Controls Reference

1. Regulatory Compliance Statement

InfiCloud affirms compliance with all applicable FCC regulations including 47 CFR § 64.6305. InfiCloud maintains an active robocall mitigation program and participates in the STIR/SHAKEN framework through its underlying network provider, Verizon Wireless.

2. STIR/SHAKEN Framework Implementation

Through Verizon's certified authentication infrastructure, complete implementation of STIR/SHAKEN is achieved.

3. Robocall Mitigation Program Overview

InfiCloud maintains proactive robocall mitigation including traffic monitoring, fraud detection, preventive subscriber screening, and enforcement actions including suspension and permanent deactivation.

4. Traffic Monitoring and Enforcement Controls

InfiCloud monitors subscriber traffic using behavioral analytics, anomaly detection, and risk-based enforcement models to detect and prevent illegal robocalling.

5. Traceback Cooperation and Contact Information

Department	Compliance and Fraud Management
Organization	InfiCloud (Infimobile)
Email	support@infimobile.com
Traceback Response Time	Within 24 hours of request

6. Certification Statement

I certify under penalty of perjury that by using Verizon Wireless's Network, Inficloud has a complete implementation of STIR/SHAKEN caller authentication and maintains a robocall mitigation program consistent with FCC regulations.

Authorized Representative: Kiran Suram Reddy

Title: CEO

Date: Feb 26, 2026

Signature:

A handwritten signature in blue ink, appearing to read "K. Suram Reddy", written in a cursive style.

Appendix A – Compliance Controls Reference

This appendix references internal mitigation policies, traffic monitoring thresholds, enforcement procedures.

1. Behavioral Threshold Model

We apply structured volume and uniqueness analytics to identify robocall and spam campaigns.

Upper Risk Tier

- ≥ 400 voice calls
- ≥ 300 SMS
- ≥ 200 unique destinations

Action:

- Immediate automated flagging
- Compliance review
- Immediate service suspension and deactivation upon confirmation

Medium Risk Tier

- ≥ 200 voice calls
- ≥ 200 SMS
- ≥ 100 unique destinations

Action:

- Elevated monitoring
- Fraud scoring escalation
- Investigation initiated

Early Warning Tier

- ≥ 100 voice calls
- ≥ 100 SMS
- ≥ 75 unique destinations

Action:

- Proactive monitoring
- Usage pattern analysis
- Risk tagging for escalation

2. Unique Destination Analysis

We specifically track the ratio of total attempts to unique destinations, which is a strong indicator of:

- Autodialer activity

- Snowshoe robocalling
- High-velocity campaign behavior

This allows InfiCloud to intervene **before consumer complaints or traceback requests occur**.

3. Pre-Activation Risk Mitigation Controls

InfiCloud enforces preventive measures at the SIM acquisition stage.

3.1 Bulk Purchase & IP Monitoring

We analyze:

- IP addresses used for SIM purchases
- Order velocity and bulk acquisition patterns
- Device/browser fingerprinting
- Payment instrument repetition
- Geographic inconsistencies

3.2 Preventive Enforcement

Where suspicious patterns are detected:

- Orders may be held for enhanced review
- Manual KYC validation may be requested
- Accounts may be denied activation
- IP sources may be restricted
- Linked accounts may be investigated

This control layer prevents bad actors from entering the network ecosystem.

4. Immediate Suspension & Zero-Tolerance Policy

InfiCloud maintains a strict enforcement posture:

- Immediate suspension upon confirmed threshold breach
- Permanent deactivation for verified robocall activity
- No reinstatement for confirmed illegal traffic
- Review of associated accounts and linked identifiers

Our objective is to minimize exposure time and eliminate abusive traffic at inception.

5. Cooperation with Verizon (MNO)

InfiCloud maintains full operational cooperation with Verizon.

5.1 MNO Deactivation Requests

Upon receiving Verizon-identified robocall or abuse notifications:

- Immediate suspension is executed
- Internal investigation is conducted
- Associated accounts are reviewed

- Pattern intelligence is integrated into detection models

We treat all Verizon enforcement actions as priority compliance matters

6. Traceback & Industry Coordination

InfiCloud supports:

- Rapid traceback response
- Timely subscriber identification (where legally permitted)
- Cooperation with industry traceback groups
- Continuous enhancement of mitigation rules based on traceback findings

7. STIR/SHAKEN Alignment

InfiCloud supports the STIR/SHAKEN framework implemented by Verizon and:

- Ensures accurate subscriber identity information
- Prevents unauthorized caller ID manipulation
- Monitors outbound traffic consistency with subscriber identity
- Investigates anomalous attestation-impacting behaviors

We recognize that improper outbound traffic may impact call attestation levels and downstream trust scoring. Our controls are designed to protect network authentication integrity.

8. Continuous Improvement & Risk-Based Governance

InfiCloud continuously:

- Reviews fraud thresholds
- Enhances traffic analytics models
- Updates IP risk controls
- Conducts internal compliance audits
- Adapts to evolving robocall tactics