

ATCVoIP LLC – Robocall Mitigation Program Description

RMD ID: RMD0008194

WC Docket No.: 17-97

File No.: EB-TCD-25-000385901

ATCVoIP LLC provides hosted VoIP services and does not directly interconnect with or terminate calls onto the public switched telephone network (PSTN). All PSTN-bound traffic is routed exclusively through upstream carrier partners (including Flowroute and Vitelity/BCM One) that have implemented STIR/SHAKEN and maintain active certifications in the FCC's Robocall Mitigation Database (RMD).

ATCVoIP is exempt from direct STIR/SHAKEN implementation pursuant to **47 C.F.R. § 64.6301(a)** because it does not originate SIP calls that are directly interconnected with the PSTN. However, ATCVoIP maintains a comprehensive robocall mitigation program consistent with **47 C.F.R. § 64.6305(d)**, including Know Your Customer (KYC) procedures, traffic monitoring, and customer enforcement mechanisms.

1. Know Your Customer (KYC) Program

ATCVoIP maintains a manual KYC program that applies to all new and existing customers. The program verifies customer identity and intended use of services prior to activation to ensure lawful calling practices.

1.1 Customer Identity Verification

Before enabling service, ATCVoIP requires each customer to provide:

- Legal business name or full personal name
- Physical address and contact information
- Valid identification details or business registration (as applicable)
- Description of intended calling use case

ATCVoIP verifies customer identity using publicly available business records and manual review of documentation. Customers who cannot be verified or whose stated use cases raise compliance concerns are not activated.

1.2 Risk-Based Assessment

Each onboarding request is reviewed for risk indicators, including:

- High-volume outbound calling
- Short-duration or predictive calling
- Telemarketing or lead generation use cases
- Requests for large blocks of DIDs or outbound-only traffic

Heightened-risk customers undergo enhanced manual due diligence prior to activation.

1.3 Existing Customer Reviews

ATCVoIP periodically reviews existing accounts to ensure continued compliance. This includes:

- Updating customer identity and contact information
- Reassessing intended use cases
- Monitoring traffic patterns for changes in risk

1.4 Planned Enhancements

ATCVoIP is developing an automated KYC workflow to strengthen both onboarding and ongoing verification. Planned improvements include:

- Automated identity verification
- Business registration validation
- Risk scoring for each new or existing account
- Automated periodic compliance review

2. Traffic Monitoring and Analytics

ATCVoIP monitors outbound call traffic for patterns associated with unlawful robocalling. Monitoring currently includes automated analysis and manual review of call detail records (CDRs).

2.1 Internal Monitoring

ATCVoIP reviews traffic for indicators including:

- High-volume short-duration calling
- Sudden spikes or abnormal changes in usage
- Repeated calls to the same destination
- Sequential or randomized dialing patterns
- Excessive calls per second (CPS)

- High call failure rates

Alerts and manual reviews occur daily. Suspicious activity is escalated immediately.

2.2 Upstream Carrier Protections

ATCVoIP's upstream carriers (Flowroute and Vitelity/BCM One) implement:

- Do-Not-Originate (DNO) protections
- Reputation scoring
- STIR/SHAKEN verification
- Blocking of invalid, unassigned, or high-risk numbers

These upstream controls provide an additional layer of defense; however, ATCVoIP does **not** rely solely on carrier-layer controls and performs internal monitoring before traffic leaves its network.

2.3 Planned Enhancements

ATCVoIP is evaluating third-party analytics tools to add real-time anomaly detection, reputation-based scoring, and additional automated alerting.

3. Investigation and Mitigation Procedures

When suspicious traffic is detected internally, reported by an upstream carrier, or identified via traceback, ATCVoIP initiates an immediate investigation.

3.1 Investigation Steps

- Review CDRs and traffic patterns
- Confirm customer identity and intended use case
- Determine whether activity violates Terms of Service
- Contact customer for additional information when needed

3.2 Mitigation Actions

Depending on findings, ATCVoIP may:

- Rate-limit or temporarily block traffic
- Disable affected DIDs
- Suspend account access
- Terminate accounts violating rules or laws

All investigations and outcomes are documented internally.

4. Cooperation with Traceback and Law Enforcement

ATCVoIP fully cooperates with the Industry Traceback Group (ITG), the FCC, and law enforcement.

ATCVoIP commits to responding to traceback requests **within 24 hours**, as required by **47 C.F.R. § 64.6305(d)(2)(iv)**.

5. Customer Terms of Service and Compliance Obligations

All customers must agree to Terms of Service prohibiting:

- Illegal robocalling
- Caller ID spoofing
- TCPA violations
- Unlawful prerecorded or autodialed calls
- Any activity prohibited by state or federal law

Violations result in immediate enforcement action, including suspension or termination.

6. Summary of Mitigation Steps

ATCVoIP's reasonable and affirmative mitigation steps include:

- Manual KYC screening for all new customers
- Periodic review of existing customers
- Monitoring for suspicious traffic patterns
- Use of upstream DNO and verification protections
- Immediate investigation of suspi