

2026 Robocall Mitigation Database Filing Narrative

Company Legal Name: Ashvoip LLC

FRN: 0035752468

OCN: 723L

Service Classifications:

Voice Service Provider, Non-Gateway Intermediate Provider, Gateway Provider

Robocall Mitigation Contact:

Name: Adam Javed

Title: Compliance officer

Email: adam@ashvoip.com

Certification

Ashvoip LLC certifies that it has fully implemented the **STIR/SHAKEN** caller ID authentication framework in the IP portions of its network and has implemented robocall mitigation practices consistent with the rules and orders of the **Federal Communications Commission**.

The company maintains policies and procedures reasonably designed to prevent customers and upstream providers from originating or transmitting illegal robocalls.

Network Description

Ashvoip LLC operates a VoIP network that originates, transits, and receives voice traffic.

The company:

- Provides interconnected voice services to customers
- Transmits traffic between telecommunications providers
- Accepts inbound international traffic directly from foreign carriers for delivery into the United States

Based on these activities the company qualifies as a:

- Voice Service Provider
- Non-Gateway Intermediate Provider
- Gateway Provider

STIR/SHAKEN Implementation

The company has deployed **STIR/SHAKEN** across the IP portions of its network.

Operational practices include:

- Authentication of outbound calls originating from known customers
- Verification of inbound authenticated calls
- Secure management of STI certificates
- Assignment of attestation levels based on the relationship with the customer and the ability to verify the right to use the calling number

Calls that cannot be authenticated due to technical limitations are subject to the robocall mitigation practices described below.

Customer and Upstream Provider Vetting

The company performs due diligence before enabling service for customers or establishing interconnection with upstream providers.

Procedures include:

- Verification of legal entity status
- Identification of business owners or responsible parties
- Review of intended use of service
- Validation of numbering resources where applicable
- Contractual prohibitions on illegal robocalling

High-risk entities may be subject to enhanced monitoring or additional verification.

Traffic Monitoring and Analytics

The company employs automated and manual monitoring systems designed to detect patterns consistent with illegal robocalls.

Monitored indicators include:

- Short duration call patterns
- Unusually high call volumes
- Sequential dialing behavior

- Invalid or unassigned numbers
- Neighbor spoofing
- Sudden spikes in traffic

Traffic determined to present a high risk of illegal robocalling may be blocked, restricted, or investigated.

Gateway Provider Protections

For inbound international traffic, the company maintains procedures designed to reduce the risk of illegal robocalls entering the United States network.

These include:

- Vetting of foreign carrier partners
- Ongoing monitoring of inbound traffic patterns
- Blocking or restricting suspicious routes
- Contractual compliance requirements for foreign providers

If notified by regulators, law enforcement, or traceback authorities that traffic is likely illegal, the company will promptly investigate and take appropriate blocking or mitigation actions.

Intermediate Provider Responsibilities

When transmitting traffic between providers, the company monitors routes and traffic patterns and will take action if it becomes aware that traffic carried on its network is associated with illegal robocalling.

Such actions may include:

- Blocking traffic
 - Suspending routes
 - Notifying upstream providers
 - Terminating service relationships where necessary.
-

Traceback Cooperation

The company cooperates with traceback investigations coordinated by the **USTelecom Industry Traceback Group** and other authorized entities.

The company responds to traceback requests within required timeframes and investigates the source of suspicious traffic identified in those requests.

Mitigation Actions

If the company determines that a customer or upstream provider is transmitting illegal robocalls, it may take actions including:

- Immediate blocking of traffic
- Suspension of service
- Termination of accounts or interconnection agreements
- Additional monitoring requirements

The company documents mitigation actions internally.

Record Retention

The company maintains records relevant to robocall mitigation activities, including:

- Customer onboarding documentation
- Traffic monitoring alerts
- Traceback responses
- Compliance investigations

These records are retained in accordance with regulatory expectations.

Compliance Oversight

Responsibility for the robocall mitigation program rests with the company's compliance function, which coordinates with network operations, legal, and management to ensure ongoing adherence to regulatory requirements and industry best practices.

The program is reviewed periodically and updated as necessary.

Certification Statement

The company certifies that the information contained in this filing is true and correct to the best of its knowledge and that it has implemented the mitigation practices described above.

Authorized Representative
Name: Muhammad Shakeel
Title: CEO
Date: 2/24/2026