



Robocall Mitigation Program Description for Mayaa LLC

Overview

Mayaa LLC relies entirely on the network infrastructure and compliance frameworks of its parent companies, **SkySwitch** and **Bandwidth**, to deliver VoIP services to its clients. These parent companies fully comply with FCC regulations, including the implementation of the STIR/SHAKEN caller ID authentication framework and robust robocall mitigation programs.

Know Your Customer (KYC)

Mayaa LLC adheres to the best practices for vetting caller identity as outlined by the NANC Call Authentication Trust Anchor Working Group. These measures ensure that all clients using the service are legitimate and do not engage in illegal robocall activities.

STIR/SHAKEN Implementation

Mayaa LLC does not perform in-house call origination or termination. Instead:

- SkySwitch and Bandwidth have fully implemented STIR/SHAKEN across portions of their networks and are compliant with 47 CFR § 64.6301(a)(1) and (2).
- Mayaa LLC relies on their certifications and infrastructures to ensure compliance with FCC regulations.

Robocall Mitigation Program

Mayaa LLC employs the following tools and practices, implemented by its parent companies:

1. **Fraud Detection:**
 - Real-time monitoring of voice traffic for high-volume robocalls, spoofing, and spam activity.
2. **Caller Authentication:**
 - Behavioral analytics and verification to ensure caller identity is legitimate.
3. **Call Blocking:**

- Systems accurately identify and block fraudulent calls as per the TRACED Act (2019).
- 4. **Subscriber Notifications:**
 - Caller ID Name overrides warn subscribers of suspicious or potentially fraudulent calls.
- 5. **Business Number Verification:**
 - Legitimate business numbers are registered to prevent unintentional blocking.
- 6. **Caller ID Services:**
 - Ensures seamless integration with caller ID lookup services and includes robocall mitigation overrides.

Traceback Compliance

Mayaa LLC and its parent companies commit to responding fully to traceback requests from:

- The FCC
- Law enforcement agencies
- The registered traceback consortium

Responses are guaranteed within 24 hours to aid in investigating and stopping illegal robocalls.

Call Abuse Policy

Any call originating on Mayaa LLC's platform is subject to inspection and investigation if deemed fraudulent, abusive, or illegal. Repeated violations may result in:

- Service disconnection
- Investigation by the FCC under the TRACED Act
- Fines and penalties imposed by regulatory authorities

STIR/SHAKEN Extensions

As a reseller with fewer than 100,000 subscriber lines, Mayaa LLC qualifies for the STIR/SHAKEN implementation extension under 47 CFR § 64.6304. All calls are subject to the robocall mitigation program detailed above.

Certification

Mayaa LLC certifies that:

1. All calls originating through its services comply with the STIR/SHAKEN framework or are subject to a comprehensive robocall mitigation program.

2. The company cooperates fully with traceback requests and enforcement actions.
 3. It relies on the parent companies' certifications for compliance with FCC rules.
-

Parent Companies

- **SkySwitch**
 - Provides the core infrastructure for call termination and origination, implementing STIR/SHAKEN compliance.
- **Bandwidth**
 - Monitors traffic and enforces the mitigation program described above.

In addition, we have implemented a Call Abuse Policy and have published the following policy to our web site, terms of use, and have notified our customers of the policy as copied below:

“Any call originated on the M Technology Solutions network is subject to inspection and investigation if the call is suspected of being fraudulent, abusive, or illegal. Calls meeting any of these criteria will be blocked. If these conditions are repeated, becoming excessive, the subscriber may be disconnected from the M Technology Solutions network, may be subject to further investigation by the FCC for enforcement of the TRACED Act and the subscriber may be subject to fines and penalties imposed by the FCC or the jurisdictional court.”

We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

Traceback

We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls.

STIR/SHAKEN Extensions

We are eligible for and are taking STIR/SHAKEN implementation extension received under 47 CFR § 64.6304 because we have fewer than 100,000 voice subscriber lines.

All the voice traffic that originates on our network is subject to the robocall mitigation program described below.

Robocall Mitigation Program

We use software provided by Bandwidth, Lumen & Peerless to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls.

Combining behavioral analytics, caller authentication and verification, our solution features:

- **Fraud Detection:** Detection of high volume robocalling, spoofing and spam call activity.
- **Subscriber Notification:** Caller ID Name override to warn subscribers of suspicious calls.
- **Call Blocking Support:** Accurate identification enabling you to block fraudulent phone calls as per the TRACED Act (2019)
- **Business Number Verification:** Register legitimate business numbers to prevent unintentional call blocking.
- **Caller ID Name Service:** Easy integration of Caller ID name lookup service, including robocall mitigation with override to include original caller ID even when call is determined fraudulent.