



Robocall Mitigation Program Description

Company Name: EMTech Services Inc.

Filer Role: Voice Service Provider Without a STIR/SHAKEN Implementation Obligation

FCC Filing Option: Option 3 - No STIR/SHAKEN Implementation

1. Overview

EMTech Services Inc. provides business VoIP services through hosted 3CX PBX systems. The Company does not obtain numbering resources directly from NANPA and does not own or operate facilities-based interconnections with the public switched telephone network (PSTN). All outbound calls are routed through the Company's underlying voice service provider, Skytel. EMTech Services Inc. maintains this mitigation program to prevent its services from being used to originate illegal robocall traffic and to comply with applicable FCC requirements.

1.1 Basis for No Direct STIR/SHAKEN Implementation

EMTech Services Inc. is not relying on an extension under 47 CFR § 64.6304. The Company has not implemented STIR/SHAKEN directly because it lacks control over the carrier systems and network infrastructure necessary to perform STIR/SHAKEN authentication and cryptographic signing.

EMTech Services Inc. provides and manages hosted 3CX PBX systems for business customers and configures Skytel SIP trunks within those systems. The 3CX PBX supplies the outbound calling number and other required SIP parameters to Skytel, but EMTech Services Inc. does not own or operate the underlying carrier network, PSTN interconnections, STIR/SHAKEN signing platform, or certificate infrastructure.

Skytel automatically signs outbound SIP INVITEs with a secure STIR/SHAKEN token when the PBX passes the required parameters. Skytel validates telephone numbers associated with the account, assigns the applicable attestation level, including A-level attestation for numbers registered to the account, and delivers authenticated calls to the

PSTN. Skyetel also processes and verifies STIR/SHAKEN Identity headers on inbound calls.

Accordingly, EMTech Services Inc. certifies to no direct STIR/SHAKEN implementation because Skyetel controls and performs the authentication, attestation assignment, cryptographic signing, certificate handling, and carrier-network functions necessary to implement STIR/SHAKEN.

2. Know Your Customer (KYC)

EMTech Services Inc. provides VoIP services only to business customers. We do not offer residential, prepaid, or anonymous calling services and we do not support high-volume mass-calling campaigns.

2.1 New Customer Onboarding

Prior to enabling call origination, all new customers undergo the following verification steps:

Business Identity Verification

- Collection of legal business name, DBA (if applicable), physical business address, and primary contact information
- Collection and validation of one or more of the following:
 - Employer Identification Number (EIN)
 - State business registration
 - Other government-issued documentation
- Verification that the customer's website and email domain align with the represented business identity

Use Case and Call Pattern Review

- Customers must provide a clear description of their intended use of the service
- The Company evaluates expected call volume, destinations, and concurrency levels for consistency with legitimate business operations
- The following use cases are explicitly prohibited:
 - Robocalling campaigns
 - Lead generation dialing
 - Bulk unsolicited outbound calling
- Any activity that may violate the TCPA or other applicable laws

Authorized Contact Verification

- The identity of the primary contact is verified through direct communication (phone or video)
- The Company confirms that the individual is authorized to act on behalf of the business

Service is not activated until all onboarding checks are successfully completed.

2.2 Application of KYC to Existing Customers

EMTech Services Inc. applies its KYC program to both new and existing customers.

- All existing customers are subject to periodic review and re-verification
- The Company is actively auditing previously onboarded customers to ensure compliance with current KYC standards
- Reviews include:
 - o Confirmation of business identity and contact information
 - o Validation of use case and calling patterns
 - o Confirmation of agreement to updated Terms of Service prohibiting illegal robocalls

If a customer fails to provide sufficient information or presents inconsistent or suspicious data:

- Service may be restricted, suspended, or terminated
- Call origination privileges may be immediately revoked until compliance is verified

2.3 Use of Analytics, Monitoring, and Upstream Providers

EMTech Services Inc. does not utilize a standalone third-party robocall analytics vendor.

However, the Company relies on the following tools and providers:

- Skyetel (underlying carrier):
 - o Provides call detail records (CDRs), fraud detection systems, and traffic monitoring tools
 - o Automatically signs outbound SIP INVITES, validates account-associated telephone numbers, and assigns the applicable STIR/SHAKEN attestation level
- 3CX PBX platform and Company monitoring tools:

- o Provide call logs, reporting, and alerting capabilities
- o Allow identification of abnormal calling behavior, including high-volume or short-duration call patterns

These systems are used to continuously monitor customer traffic and identify potential indicators of illegal robocalling.

2.4 Enforcement and Ongoing Compliance

KYC is not a one-time process. All customers are subject to continuous monitoring and enforcement.

If suspicious or potentially illegal activity is detected:

- The Company will immediately review call records and account activity
- The customer will be contacted to provide an explanation
- Traffic may be:
 - Blocked
 - Rate-limited
 - Temporarily disabled

If the activity is determined to be illegal or the customer fails to cooperate:

- Service will be suspended or terminated
- The customer will not be allowed to resume service until compliance is confirmed

3. Traffic Monitoring and Mitigation

3.1 Ongoing Monitoring

- Sudden spikes in call volume.
- High volumes of short-duration calls.
- Repeated calling to the same destinations.
- Patterns consistent with robocalling.
- Complaints or traceback notices.

3.2 Reasonable Steps to Mitigate Illegal Traffic

Immediate Review:

- Review call detail records.
- Compare activity with expected patterns.

Customer Contact:

- Notify customer and request explanation.
- Remind customer of legal obligations.

Traffic Control Measures:

- Block suspicious prefixes or numbers.
- Rate-limit outbound calls.
- Disable offending trunks.

Escalation:

- Suspend or terminate service for non-cooperative customers.
- Restore service only when issue is mitigated.

4. Cooperation with Traceback and Enforcement

- Respond to traceback requests within 24 hours.
- Provide all information needed to identify the source of suspicious traffic.

5. Conclusion

EMTech Services Inc. does not directly implement STIR/SHAKEN because it lacks control over the carrier systems and infrastructure required to perform authentication and cryptographic signing. Skytel performs those carrier-side functions. EMTech Services Inc. remains responsible for customer vetting, traffic monitoring, mitigation, and traceback cooperation. These controls are designed to prevent the Company's services from being used to originate or transmit illegal robocall traffic.