

Robocall Mitigation Program Description

FCC Robocall Mitigation Database Filing - PDF Upload Document

1. Filer / Company Information

Legal Company Name	Digitech Solutions, Inc.
Doing Business As / DBA	
FCC Registration Number (FRN)	0027553205
Robocall Mitigation Database Filing Type	Initial Filing
Company Website	www.digitech.net
Principal Business Address	147 Waverly Drive, Pasadena, CA 91105
Compliance Contact	Michael Nehme, CEO, 8189834949, michael@digitech.net

2. Provider Role and Service Description

The filer should identify its role in the voice call path and describe the services it provides. Select all roles that apply and provide a concise explanation of the company's voice services, customers, traffic sources, and network relationships.

☒ Voice Service Provider / Originating Provider	☐ Gateway Provider
☐ Intermediate Provider	☐ Non-Facilities-Based Provider / Reseller
☐ Wholesale Provider	☐ Enterprise / Call Center Service Provider
☐ Other: [describe]	

Service Description: Digitech Solutions, Inc. resells VoIP/SIP services through CoreNexa and relies on CoreNexa for STIR/SHAKEN authentication, call attestation, STI-AS/STI-VS functions, certificate authority access, and implementation in the IP voice network.

3. STIR/SHAKEN Implementation Status

Digitech Solutions, Inc. resells VoIP/SIP services through CoreNexa and relies on CoreNexa for STIR/SHAKEN authentication, call attestation, STI-AS/STI-VS functions, certificate authority access, and IP voice network implementation.

☒ Fully implemented STIR/SHAKEN in applicable IP network portions
☐ Partially implemented STIR/SHAKEN - describe implementation scope and remaining gaps
☐ Not implemented / not applicable - describe basis and mitigation steps used instead

Implementation Details: Digitech Solutions, Inc. resells VoIP/SIP services through CoreNexa. Digitech does not directly operate STI-AS/STI-VS infrastructure, does not directly obtain STI certificates from a Certificate Authority, and does not directly assign numbering resources. STIR/SHAKEN authentication, Certificate Authority access, STI-AS/STI-VS functionality, numbering resources, and final attestation decisions are handled by CoreNexa and/or its applicable underlying carrier network. Digitech does not independently provide A-level attestation. Final attestation is determined by CoreNexa and/or the applicable underlying carrier based on their STIR/SHAKEN policies, customer relationship, telephone number assignment, and verification of the customer's right to use the calling number. Digitech's customer authorization controls include verifying customer identity and business legitimacy where applicable, maintaining customer account records, confirming that customers are authorized to use assigned or presented telephone numbers, and prohibiting spoofing, fraudulent calls, unlawful robocalls, and manipulation of caller ID information. Customers may only originate calls using numbers assigned to them or numbers they are legally authorized to use. Digitech coordinates with CoreNexa regarding suspicious or abusive calling activity. If suspected illegal robocalling, spoofing, fraud, or unauthorized caller ID use is identified, Digitech may investigate, request documentation, restrict service, suspend service, terminate service, and/or escalate the matter to CoreNexa. Limitations: Digitech does not control CoreNexa's STIR/SHAKEN platform, Certificate Authority relationship, STI-AS/STI-VS systems, final attestation level, numbering assignments, call analytics, call blocking, or carrier-level mitigation tools. Digitech will cooperate with CoreNexa, traceback requests, carrier investigations, law enforcement requests, and FCC inquiries as applicable.

4. Robocall Mitigation Program Overview

Digitech Solutions, Inc. maintains a robocall mitigation program to prevent, detect, investigate, and respond to illegal robocalls and caller ID spoofing. Digitech resells VoIP/SIP services through CoreNexa and relies on CoreNexa for carrier-level STIR/SHAKEN, call attestation, numbering resources, and network mitigation controls. Digitech verifies customers, requires authorized number use, reviews suspicious activity, and may restrict, suspend, terminate, or escalate service issues to CoreNexa when misuse is identified.

Program Element	Description / Controls
Prevention	Digitech Solutions, Inc. vets customers where applicable, maintains customer account records, requires authorized use of telephone numbers, prohibits unlawful robocalls and caller ID spoofing, and relies on CoreNexa for carrier-level STIR/SHAKEN and mitigation controls.
Detection	Digitech monitors customer activity to the extent visible through its reseller relationship, reviews complaints or fraud alerts, and coordinates with CoreNexa regarding suspicious traffic, traceback requests, or abnormal calling activity.
Investigation	Digitech reviews suspicious traffic, customer complaints, traceback requests, and law enforcement inquiries. Issues may be escalated internally and to CoreNexa for carrier-level investigation and mitigation.
Response	Digitech may warn customers, request supporting documentation, restrict service, suspend service, terminate service, or escalate issues to CoreNexa when suspected illegal robocalling, spoofing, or fraud is identified.
Recordkeeping	Digitech maintains customer account records, service records, complaint records, investigation notes, traceback-related records, and corrective action documentation as applicable.

5. Know-Your-Customer and Customer Due Diligence

Digitech Solutions, Inc. verifies customer identity and business legitimacy where applicable before providing VoIP/SIP services. Digitech confirms customer contact information, service address, authorized representatives, and the customer's right to use requested telephone numbers or caller ID information. Customers are required to comply with applicable robocall, caller ID, TCPA, Truth in Caller ID, and anti-fraud requirements. Digitech may review higher-risk customers, including high-volume callers, call centers, lead generation customers, or customers using automated dialing. Digitech may suspend, restrict, or terminate service for suspected unlawful traffic or failure to cooperate with investigations.

6. Traffic Monitoring and Suspicious Traffic Detection

Digitech Solutions, Inc. monitors customer activity to the extent visible through its reseller relationship with CoreNexa. Digitech reviews complaints, fraud alerts, traceback requests, unusual calling patterns, unauthorized caller ID use, and reports from CoreNexa or other carriers. Suspicious traffic may be escalated to CoreNexa for carrier-level review, mitigation, blocking, or further investigation.

Detection Signal	Example Review Criteria
High call volume or spikes	Unexpected traffic increases, short-duration call bursts, repeated unanswered calls, abnormal answer seizure ratio, or volume inconsistent with customer profile.
Caller ID anomalies	Use of unauthorized numbers, invalid numbers, unassigned numbers, numbers not associated with the customer, or repeated caller ID changes.
Complaint indicators	Consumer complaints, carrier notices, traceback requests, enforcement communications, or spam-labeling feedback.
Destination / routing patterns	Unusual destination mix, repeated short calls, traffic to high-risk destinations, or patterns associated with fraud campaigns.

7. Complaint, Traceback, and Law Enforcement Response

Digitech will review complaints, traceback requests, law enforcement requests, and FCC inquiries, coordinate with CoreNexa when needed, and take corrective action such as restricting, suspending, or terminating service if misuse is found.

Step	Procedure
Intake	Record the date, source, contact, affected numbers, call examples, and any deadline for response.
Review	Match complaint details to customer records, call detail records, routing data, STIR/SHAKEN information, and account activity.
Customer Outreach	Contact the responsible customer or provider, request explanation and supporting documentation, and require immediate remediation where appropriate.
Corrective Action	Block numbers, restrict traffic, suspend service, terminate service, notify upstream/downstream partners, or take other steps based on risk and evidence.
Documentation	Maintain records of the request, analysis, communications, action taken, and closure status.

8. Upstream and Downstream Provider Controls

Digitech Solutions, Inc. resells VoIP/SIP services through CoreNexa and relies on CoreNexa and its underlying carrier network for carrier-level voice traffic controls. Digitech maintains provider contact information, cooperates with traceback and abuse investigations, and may restrict or discontinue services involving suspicious or unlawful traffic. Digitech does not knowingly accept or support traffic from unauthorized or non-compliant providers.

9. Blocking, Suspension, and Termination Procedures

Digitech may warn customers, request documentation, restrict calling, suspend service, terminate service, or escalate the issue to CoreNexa based on the severity and evidence of suspected unlawful robocalling, spoofing, fraud, or abuse. Urgent matters, traceback requests, carrier complaints, law enforcement requests, or FCC inquiries are escalated to Digitech management and CoreNexa as needed.

Escalation Matrix:

Suspicious or unlawful traffic is reviewed by Digitech technical/management staff and escalated to CoreNexa when carrier-level action is required. Corrective actions may include customer warning, service restriction, suspension, termination, or cooperation with regulatory or law enforcement requests.

10. Recordkeeping and Compliance Governance

Digitech maintains customer records, service records, number authorization information, complaint records, traceback responses, investigation notes, and corrective action documentation as applicable.

Retention Period:

Records are retained for at least two years, or longer if required by law, contract, investigation, or regulatory request.

Program Review:

Digitech reviews its robocall mitigation program at least annually and updates it as needed based on customer activity, provider requirements, FCC rules, traceback requests, complaints, or operational changes.

11. Confidentiality / Redaction Instructions

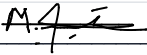
If confidential treatment is requested, Digitech will prepare a confidential unredacted version and a public redacted version of this document. The public version will remove sensitive business, vendor, network, security, escalation, and operational details. If no confidential treatment is requested, Digitech will upload one non-confidential PDF version.

12. Compliance Statement

Digitech Solutions, Inc. maintains a robocall mitigation program designed to prevent illegal robocalls, unlawful spoofing, fraud, and abusive calling activity. Digitech will cooperate with CoreNexa, traceback requests, carrier complaints, law enforcement requests, and regulatory inquiries, and will take corrective action when suspicious or unlawful traffic is identified.

13. Certification / Signatory Information

The information in this Robocall Mitigation Program Description is certified as accurate and complete to the best of the signer's knowledge. The authorized representative of Digitech Solutions, Inc. certifies that the company maintains and follows the robocall mitigation procedures described in this document.

Certifying Official Name	Michael Nehme
Title	CEO
Company	Digitech Solutions, Inc.
Phone	818-983-4949
Email	michael@digitech.net
Signature	
Date	06/12/26

Prepared as a template for FCC Robocall Mitigation Database filing support. This document does not constitute legal advice.