ROBOCALL MITIGATION PLAN

Vertex Logics LLC

FCC Registration Number (FRN): 0039018353
FCC Form 499 Filer ID: 839421
Operating Company Number (OCN): Pending
State of Organization: Montana, United States
Effective Date: October 29, 2026
Version: 1.0

1. Purpose and Scope

Vertex Logics LLC ("Company") is a United States-based provider of retail Voice over Internet Protocol ("VoIP") services to business end users. The Company also acts as a gateway provider with respect to certain foreign-originated voice traffic entering the United States.

The Company has adopted this Robocall Mitigation Plan to establish reasonable and effective policies, procedures, and controls designed to prevent, detect, investigate, and mitigate illegal robocalls and unlawful Caller ID spoofing involving the Company's services or network.

The Company's robocall mitigation program includes:

- customer identification and Know Your Customer ("KYC") procedures;
- customer risk assessment;
- telephone number and Caller ID controls;
- STIR/SHAKEN implementation;
- monitoring of voice traffic;
- gateway provider controls;
- traceback cooperation;
- investigation of suspicious traffic;
- customer warning, suspension, and termination procedures;
- complaint management;
- upstream and foreign-provider due diligence; and
- periodic compliance review.

The Company implements and follows the procedures described in this Plan as part of its ongoing robocall mitigation program.

The FCC Public Notice on RMD filing requirements states that mitigation plans must describe the provider's specific reasonable steps to avoid originating, carrying, or processing illegal robocall traffic.

2. Company Operations and Provider Classification

The Company provides retail VoIP services directly to business end-user customers. The Company does not provide retail VoIP services to individual consumers.

Business customers may originate outbound calls using the Company's services.

The Company does not operate as a wholesale voice provider accepting voice traffic from unrelated domestic VoIP providers for resale or transit.

In addition to its retail voice service operations, the Company acts as a **Gateway Provider** with respect to traffic received directly from foreign originating or foreign intermediate providers and transmitted into the United States through the Company's applicable U.S.-based facilities.

The FCC RMD FAQ defines a gateway provider as a U.S.-based intermediate provider receiving a call directly from a foreign provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider.

The Company does **not** act as a non-gateway intermediate provider based upon its current operations.

The Company currently has no parent company, subsidiaries, or affiliates.

3. STIR/SHAKEN Implementation

The Company has implemented STIR/SHAKEN functionality for applicable SIP traffic on the IP portions of its network.

The Company's own STI certificate is presently pending. Until the Company's own certificate becomes available and operational, STIR/SHAKEN authentication is performed through the Company's existing technical and carrier arrangements.

Once its own STI certificate becomes available and is integrated into the Company's authentication infrastructure, the Company will use the certificate consistent with applicable STIR/SHAKEN requirements and its technical implementation.

The Company will not represent in its Robocall Mitigation Database filing that it currently signs calls using its own STI certificate until the certificate has been issued and implemented.

The FCC states that voice service providers and gateway providers are among the provider types required to implement STIR/SHAKEN, subject to the applicable rules and any available extensions.

Current Attestation Practices

The Company currently applies or causes **B-level attestation** to be applied to applicable outbound traffic based on its authenticated relationship with the customer.

The Company knows and verifies the identity of the business customer originating the call.

The Company does not intentionally provide an attestation level that represents knowledge or authorization the Company does not possess.

The Company will periodically evaluate its attestation practices as its STIR/SHAKEN implementation and certification arrangements develop.

4. Know Your Customer Program

The Company applies KYC procedures to business customers before permitting them to originate outbound voice traffic.

The purpose of the KYC process is to:

1. reasonably establish the customer's identity;
2. verify that the customer is a legitimate business;
3. understand the customer's intended use of the Company's voice services;
4. evaluate the risk associated with the customer and its proposed calling activity; and
5. reduce the likelihood that Company services will be used for illegal robocalling, fraud, or unlawful spoofing.

The Company does not currently provide service to individual consumer customers.

4.1 Business Customer Information

As applicable to the particular customer and risk profile, the Company collects and evaluates information including:

- legal business name;

- DBA or trade name, if applicable;
- state or jurisdiction of organization;
- business registration information;
- Employer Identification Number or other applicable tax/business identification information;
- physical business address;
- telephone number;
- business email address;
- company website/domain;
- name of the owner or authorized representative;
- government-issued identification of the responsible or authorized individual;
- nature of the customer's business;
- intended use of the Company's VoIP services;
- expected calling activity; and
- other information reasonably necessary to evaluate the legitimacy of the customer.

4.2 Verification

The Company verifies relevant business information using documentation and reliable information available to it.

Depending upon the customer's circumstances and risk profile, the Company may require additional documentation or clarification before service activation.

The Company may reject an application where it cannot reasonably establish the customer's identity, business legitimacy, or legitimate purpose for obtaining voice services.

5. Customer Risk Assessment

Customer due diligence does not end upon account activation.

The Company evaluates relevant information throughout the customer relationship and may subject a customer to enhanced review where indicators of potentially unlawful or abusive calling activity are identified.

Relevant risk indicators may include:

- unusual increases in outbound traffic;
- calling patterns materially inconsistent with the customer's stated business;
- unusually high volumes of short-duration calls;
- suspicious Caller ID patterns;
- complaints concerning the customer's calls;
- traceback requests associated with the customer's traffic;
- reports from carriers concerning suspicious traffic;
- suspected Caller ID spoofing; or
- other activity indicating potential misuse of the Company's services.

Customers presenting elevated risk may be required to provide additional supporting information.

6. Telephone Number and Caller ID Controls

The Company obtains telephone numbers/DIDs from established telecommunications and numbering vendors and assigns those numbers to its customers as appropriate.

Customers are expected to originate calls using telephone numbers that have been assigned or otherwise authorized for their legitimate use.

Customers may not knowingly transmit false, misleading, or unauthorized Caller ID information for unlawful or deceptive purposes.

The Company may investigate circumstances where:

- the calling number is not reasonably associated with the customer;
- unusual Caller ID patterns are identified;
- potentially unauthorized telephone numbers are used;
- spoofing is suspected; or
- a complaint, traceback, or carrier notification calls the customer's number usage into question.

Where necessary, the Company may require supporting evidence demonstrating the customer's authorization to use particular telephone numbers.

7. Customer Acceptable Use and Contractual Controls

Customers are prohibited from using the Company's network or services to engage in illegal calling activity.

Prohibited activity includes use of Company services for:

- illegal robocalling;
- fraudulent or deceptive calling campaigns;
- unlawful Caller ID spoofing;
- impersonation or misrepresentation for unlawful purposes;
- transmission of calls in violation of applicable telecommunications or consumer-protection requirements;
- attempts to evade call authentication, blocking, monitoring, or traceback mechanisms; or
- other unlawful use of telecommunications services.

The Company's contractual arrangements permit the Company, as appropriate, to:

- investigate suspicious activity;
- request documents and explanations from customers;
- monitor potentially abusive traffic;
- restrict calling activity;
- block or reject prohibited traffic;
- suspend services; and
- terminate customers involved in prohibited activity.

8. Traffic Monitoring and Analytics

The Company utilizes the **PeerEdge platform provided by 46 Labs** as part of its voice switching and traffic management infrastructure. The platform provides the Company with access to call detail records, traffic information, reporting, and other operational information used to monitor voice traffic and investigate potentially suspicious calling activity.

Company personnel use information available through PeerEdge, together with customer KYC information, carrier notifications, complaints, traceback requests, and other relevant information, to identify and investigate potentially unlawful or abusive calling activity.

The Company's monitoring may include review of:

- inbound and outbound call detail records;
- calling and called telephone numbers;
- call duration and volume;
- SIP response information;
- originating and terminating connections or trunks;
- unusual or repetitive calling patterns;
- Caller ID anomalies;
- material changes in customer traffic;
- traffic inconsistent with the customer's known business purpose;
- traceback requests;
- consumer or carrier complaints; and
- other indicators reasonably suggesting potentially unlawful or abusive activity.

PeerEdge documentation specifically confirms CDR searches by direction, connection, ANI, dialed number and date/time, with results containing information including SIP codes, duration and connection information.

Where monitoring identifies suspicious activity, the Company may conduct further investigation using available CDRs, customer KYC information, telephone-number assignments, STIR/SHAKEN information, carrier information, and other relevant records.

Where appropriate, the Company may request an explanation or supporting documentation from the customer and may apply enhanced monitoring, traffic restrictions, warnings, suspension, blocking, or termination in accordance with this Robocall Mitigation Plan.

9. Gateway Provider Mitigation

Because the Company acts as a gateway provider for certain foreign-originated traffic entering the United States, it maintains additional measures applicable to such traffic.

The Company conducts reasonable due diligence regarding providers from which it directly receives applicable foreign-originated traffic.

Depending upon the relationship and associated risk, the Company's review may include:

- legal identity of the provider;
- business address and contact information;
- regulatory information reasonably available to the Company;
- Robocall Mitigation Database status where applicable;
- expected nature and volume of traffic;
- STIR/SHAKEN practices where applicable;
- representations concerning lawful traffic;
- traceback history or other identified abuse; and
- information concerning the provider's relationship with the Company.

Foreign-originated traffic may be subject to monitoring and investigation where patterns indicate possible illegal robocalling, spoofing, fraud, or other abuse.

Where the Company's investigation identifies unacceptable risk or potentially unlawful traffic, the Company may restrict, block, suspend, or terminate the relevant traffic or provider relationship as appropriate.

The FCC describes gateway providers as the entry point for qualifying foreign calls into the United States and has required gateway providers to implement robocall mitigation programs.

10. Know Your Upstream Provider Procedures

The Company obtains telecommunications connectivity from established upstream carriers and conducts reasonable due diligence appropriate to these relationships.

The Company may consider information including:

- provider identity;
- FCC registration information;
- RMD registration/status where applicable;
- nature of services provided;
- STIR/SHAKEN practices;
- operational and compliance contacts; and
- relevant compliance representations.

The Company does not knowingly maintain an upstream relationship for the purpose of facilitating illegal robocall traffic.

11. Investigation of Suspicious Traffic

Potentially unlawful or abusive voice traffic is escalated to appropriate Company personnel for investigation.

An investigation may include review of:

- KYC documentation;
- customer account information;
- relevant call detail records;
- calling and called numbers;
- Caller ID information;
- traffic volumes;
- calling patterns;
- complaints;
- traceback information;
- available STIR/SHAKEN information;
- carrier reports; and
- explanations and supporting information provided by the customer.

The Company may require a customer to provide information reasonably necessary to establish the legitimate purpose of questioned traffic.

Failure to provide an adequate explanation or supporting documentation may result in restrictions, suspension, or termination.

12. Warning, Suspension and Termination

The Company maintains an escalation procedure for customer violations and suspicious activity.

First Warning

For conduct warranting corrective action, the Company may issue an initial warning requiring the customer to explain the traffic and correct the identified issue.

Second Warning

Where the problematic activity continues, recurs, or is not satisfactorily explained, the Company may issue a final warning and require immediate remediation.

Additional monitoring or traffic restrictions may also be imposed.

Suspension or Termination

Following two warnings, if the problematic activity continues or remains inadequately explained, the Company may suspend the customer's outbound calling capability or terminate service.

Immediate Enforcement

The Company's two-warning process does **not** require the Company to permit seriously suspicious or apparently unlawful traffic to continue.

The Company reserves the right to immediately restrict, block, suspend, or terminate service without prior warning where available information demonstrates or reasonably indicates serious unlawful, fraudulent, deceptive, harmful, or abusive activity, or where immediate intervention is reasonably necessary to protect consumers, telecommunications networks, the Company, its carrier partners, or the integrity of the Company's services.

13. Industry Traceback Group and Traceback Cooperation

The Company cooperates with legitimate traceback requests concerning suspected illegal robocall traffic.

The Company is committed to **responding fully to traceback requests from the FCC, law enforcement, and the Industry Traceback Consortium within 24 hours**, as required by the applicable robocall mitigation framework. The FCC identifies this commitment as part of providers' mitigation obligations.

Upon receipt of a traceback request, responsible personnel use available:

- call detail records;
- telephone number information;
- customer records;
- routing information;
- carrier information; and
- other relevant network information

to investigate the call.

Where traceback activity identifies potentially unlawful traffic associated with a Company customer or provider relationship, the Company conducts further investigation and may take corrective action.

Such action may include monitoring, warning, traffic restrictions, suspension, blocking, or termination as appropriate.

14. Consumer and Carrier Complaints

Complaints concerning suspected illegal robocalls, spoofing, fraud, or misuse of Company services are escalated for review.

Where sufficient call information is available, the Company may:

1. identify relevant call records;
2. identify the responsible customer or traffic source;
3. examine calling patterns and Caller ID information;
4. review the customer's KYC information;
5. request additional information from the customer;
6. determine whether remedial action is required; and

7. document material action taken.

Multiple or substantiated complaints may result in enhanced monitoring, restriction, suspension, or termination.

15. Regulatory and Law Enforcement Cooperation

The Company cooperates in good faith with the Federal Communications Commission, appropriate law enforcement authorities, the Industry Traceback Consortium, telecommunications providers, and other appropriate entities investigating suspected illegal robocalls or unlawful spoofing involving the Company's services.

16. Recordkeeping

The Company maintains records reasonably necessary to operate, document, and evaluate its robocall mitigation program.

Such records may include:

- customer KYC documentation;
- onboarding and verification information;
- telephone number assignments;
- relevant call detail records;
- customer communications;
- traceback requests and responses;
- complaints;
- investigations;
- customer warnings;
- suspensions;
- terminations;
- carrier communications; and
- other documentation associated with material robocall mitigation activity.

Records are maintained and protected consistent with applicable legal, regulatory, contractual, operational, privacy, and security requirements.

17. Compliance Oversight

Personnel involved in customer onboarding, compliance, network operations, fraud prevention, and carrier management are expected to escalate indications of suspected illegal robocall activity to the appropriate responsible personnel.

Material incidents may be reviewed by Company management to determine whether customer-specific corrective measures or broader changes to Company controls are appropriate.

The Company expects personnel responsible for implementation of this Plan to apply the Company's mitigation procedures consistently.

18. Periodic Review

The Company periodically evaluates the effectiveness of its robocall mitigation program.

The Company considers factors including:

- traceback activity;
- complaints;
- identified abuse;
- changes in customer traffic patterns;
- network and service changes;
- STIR/SHAKEN implementation;
- experience with foreign-originated traffic;
- carrier relationships; and
- applicable regulatory developments.

The Company may modify its policies, procedures, monitoring, or contractual requirements when appropriate to address identified risks.

The Company will update information contained in its Robocall Mitigation Database filing when required.

19. Management Commitment

Vertex Logics LLC is committed to taking reasonable and effective measures to prevent its services and network from being used for illegal robocalling, unlawful spoofing, fraud, or other prohibited calling activity.

The Company implements the specific practices described in this Robocall Mitigation Plan as part of its ordinary operations and will continue to evaluate and improve its mitigation controls as its business and network develop.

Authorized Representative

Name: _____Muhammad Kashif Shahzad____

Title: _____CEO_____

Company: Vertex Logics LLC

Signature: _____Kashif Shahzad_____

Date: _____October 29, 2026_____