

Vaspian LLC

Robocall Mitigation Plan

Background

Under the authority Congress granted the Federal Communications Commission (“FCC” or “Commission”) in the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, the Commission has adopted rules requiring voice service providers, like Vaspian LLC. (“Vaspian”), to implement STIR/SHAKEN caller ID authentication technology in the Internet Protocol (IP) portions of their networks. 47 CFR § 64.6301.

The FCC requires that all voice service providers certify, by September 28, 2021, in the Commission’s Robocall Mitigation Database whether they have implemented STIR/SHAKEN or, if subject to an applicable extension, that they have documented and instituted a robocall-mitigation plan to help combat the origination of illegal robocalls on their networks. The Commission has explained that a robocall-mitigation program is sufficient if the detailed practices in the plan can “reasonably be expected to significantly reduce the origination of illegal robocalls” and the voice service provider complies with the practices it describes in its filings.

Vaspian is dedicated to stopping illegal calls from originating on its network and undertaking commercially reasonable efforts to monitor the calls coming into its network, consistent with FCC regulations and its “Best Practices” guidance.

This document outlines Vaspian’s Robocall Mitigation plan.

Vaspian’s “Know Your Customer” Standards

Vaspian is a hosted voice service provider that focuses its business and operations on the small to medium size customer segments of the voice services communications market. As part of its customer-onboarding process, Vaspian undertakes various commercially reasonable precautions to verify a given prospective customer’s identity and relevant business practices as part of entering into a formal written agreement with that customer. All prospective customers must complete a questionnaire which provides Vaspian with detailed background corporate information about the customer. This questionnaire solicits vital information, such as:

1. Name of contact person responsible for account, and the name of the person responsible for payment;
2. Customer’s state or country of incorporation;
3. Description of the nature of the customer’s business;
4. The customer’s federal taxpayer identification number or equivalent;
5. Customer’s billing address and all addresses at which customer conducts business;
6. If the customer is a reseller, we do not provide service. Vaspian only deals directly with customers or agents;

Vaspian's Acceptable Use Policy (AUP)

As part of its customer-onboarding process, Vaspian's customers contractually agree to various terms and conditions, including a commitment to comply with Vaspian's Terms of Use. Among other things, these Terms prohibit:

- Using the Services to engage in any activities that are illegal, abusive, false, fraudulent, deceptive or misleading, or any activity that exploits, harms, or threatens to harm children.
- Engaging in any unsolicited advertising, marketing, or other unlawful activities using the Services that violate laws applicable to advertising, electronic communications, and telemarketing, including, but not limited to, Section 5 of the FTC Act (15 U.S.C. § 45), the CAN-SPAM Act (15 U.S.C. §§ 7701-7713), the Telemarketing Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108), the Federal Trade Commission Telemarketing Sales Rule (16 C.F.R. § 310 et seq.), the Telephone Consumer Protection Act (47 U.S.C. §§ 227), the Federal Communications Commission regulations (47 C.F.R. 64.1200 et seq.) and orders implementing the Telephone Consumer Protection Act, and all federal and state Do Not Call and calling-time restriction laws and regulations.
- Using Vaspian LLC's Services in any way that fails to conform to any applicable industry guidelines and standards, including, without limitation, the CTIA Messaging Principles and Best Practices, Short Code Registry Best Practices, and Short Code Monitoring Handbook.
- Creating a false identity, forged email address or header, phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or phone call, including failing to comply with the Truth in Caller ID Act.
- Vaspian customers have confirmed they have written consent to contact all end user telephone numbers.

Vaspian's contracts with its customers stipulate that it is authorized to suspend and/or terminate all Services in the event of an AUP violation

Telephone Number Authorization and STIR-SHAKEN Capabilities

Vaspian has adopted the STIR/SKAKEN framework for verifying the authenticity of a caller's phone number using digital certificates and encryption and is in full compliance.

Proactive Network Monitoring

Vaspian has various monitoring and reporting systems in place to analyze traffic on its network for potentially suspicious traffic patterns that are likely to be associated with illegal robocalls or other potentially unlawful usage. For example, Vaspian's monitoring systems are capable of assessing traffic based on various criteria, including data relating to short-duration calls, answer-seizure ratios, invalid Caller ID ANIs, and anomalous volumes of 404, 503 and other call-failure codes.

If Vaspian detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, Vaspian takes prompt action to identify the party that is using its network to carry these calls and take appropriate action. Once suspected unlawful traffic is discovered, Vaspian blocks any further traffic from the customer and issues an Acceptable Use Violation notice.

Commitment to Traceback Cooperations

Vaspian commits to timely cooperation with, and responding to within 24 hours, Traceback requests from the ITG (or any successor entity designated by the FCC), trace-forward investigations, and other valid law enforcement and government demands, subpoenas, and other valid legal processes.

Vaspian will dedicate sufficient resources to provide prompt and complete responses to such requests. Vaspian will investigate suspicious activity found by its monitoring systems or reported to it by consumers or third parties and take appropriate action.