



ROBOCALL MITIGATION PLAN

By:
HAZTEL INC. Tech Team

Program Lead:
Zubair Salahuddin
Director Carrier Relations

April 28th 2024

A. Background

HAZTEL INC. ROBOCALL MITIGATION PLAN

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 HAZTEL INC. (“HAZTEL INC.”), 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 June 30, 2021, in the Commission’s Robocall Mitigation Database (RMD) i.e. https://fccprod.servicenowservices.com/rmd?id=rmd_welcome 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.

HAZTEL INC. 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 practice guidance.

Ref: <https://docs.fcc.gov/public/attachments/DA-20-1526A1.pdf>

This document briefs HAZTEL INC.’s Robocall Mitigation plan.

B. HAZTEL INC.’s KYC (Know Your Customer) SOPs

HAZTEL INC. is a new retail, intermediate voice service provider that focuses its business and operations on the retail voice services in communications market.

As part of its customer- onboarding process, HAZTEL INC. undertakes various commercially reasonable precautions to verify a given customer’s identity, including having its customers complete a KYC questionnaire, a USF Exemption Certificate, and a formal written contract.

Among other data points collected and, as appropriate, verified, as part of those processes HAZTEL INC. gathers the following customer-identifying facts and circumstances:

- Customer Business Name,
- State or Country of Incorporation,
- Physical Business Location,
- Contact Person(s),
- Federal Tax ID Number, and
- FCC Filer ID.

HAZTEL INC.'s enhanced verification practices include:

- Confirming a carrier customer's reported status in the FCC's Form 499 Filer database of registered carriers, and, as of June 30, 2021, the Commission's Robocall Mitigation Database.
- HAZTEL INC. also conducts, as applicable, credit checks and check trade references with a prospective customer's other carrier-suppliers.

C. HAZTEL INC.'s Acceptable Use Policy

As part of its customer-onboarding process, all of HAZTEL INC.'s customers contractually agree to various terms and conditions, including a commitment to comply with HAZTEL INC.'s Acceptable Use Policy (AUP). Among other things, this AUP prohibits:

- 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, including, without limitation, any activities 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 HAZTEL INC.'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.

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

D. Telephone Number Authorization and STIR-SHAKEN Capabilities

As noted above, HAZTEL INC. provides its intermediate voice services solely to other registered originating and intermediate voice service providers. As such, HAZTEL INC. is not the originating provider capable of authenticating the calling party's relationship with the caller ID ascribed to a given call. HAZTEL INC.'s network is, however, already capable of accepting and accurately transmitting all STIR-SHAKEN-related data it receives in the call path.

E. Efficient/Stay-Alert Network Monitoring

HAZTEL INC. 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 and frauds.

For example, HAZTEL INC.'s monitoring systems assess and, as applicable, flag or automatically block, traffic based on various criteria, including

- Matching NPA-NXXs of the calling and called parties' telephone numbers;
- Calls with a caller ID of a telephone number associated with a wireless carrier from a customer understood not to carry wireless-originated traffic;
- Blocking calls for which the caller ID is not a valid, in- service ANI in the LERG;
- Blocking calls from any Media IP address associated with a known or reported illegal robocalling entity; and
- using ASR tool to block calls—typically very short duration calls—likely associated with DDOS attacks.

If HAZTEL INC. detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, HAZTEL INC. takes prompt action to identify the party that is using its network to carry these calls and take appropriate action.

F. Complying Commitment to Traceback Cooperation (CCTC)

HAZTEL INC. commits to timely cooperating with and responding to 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. HAZTEL INC. will dedicate sufficient resources to provide prompt and complete responses to such requests. HAZTEL INC. will investigate suspicious activity found by its monitoring systems or reported to it by consumers or third parties and take appropriate action.