

HAWAIIAN TELCOM, INC.
HAWAIIAN TELCOM SERVICES COMPANY, INC.
WAVECOM SOLUTIONS CORP.
SYSTEMMETRICS CORPORATION

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 C.F.R. § 64.6305, Hawaiian Telcom, Inc. (“HTI”), Hawaiian Telcom Services Company, Inc. (“HTSC”), Wavecom Solutions Corp. (“Wavecom”) and SystemMetrics Corporation (“SystemMetrics”) (collectively, “Hawaiian Telcom”) submit this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. Hawaiian Telcom reserves the right to modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time as it deems appropriate to reflect its business, its capabilities, and its needs.

Company Background

HTI is the incumbent local exchange carrier in Hawaii, providing voice and data services to residential and business customers throughout the state. Wavecom is a competitive local exchange carrier offering local telephone service to business customers Hawaii. HTSC offers long distance, broadband Internet access service, and video service to residential and business customers in Hawaii, and business VoIP solutions. SystemMetrics offers IP services to businesses in Hawaii.

Hawaiian Telcom primarily exchanges traffic via TDM, although it does have the ability for IP interconnection for a small portion of its traffic which will utilize the STIR/SHAKEN framework. The non-IP portions of its network qualify for the non-IP exception for implementation of STIR/SHAKEN. As described below, Hawaiian Telcom has implemented a Robocall Mitigation Program for its entire operation and Hawaiian Telcom has deployed protections designed to ensure that it remains free of illegal robocalls on its network.

Hawaiian Telcom has not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action, and none of its prior certifications have been removed from the Database by the Commission.

Hawaiian Telcom has not been, at any time in the prior two years, the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to it transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description. The same is true for any entities affiliated with Hawaiian Telcom.

Hawaiian Telecom's OCNs are 3100 for Hawaiian Telecom, Inc., 009G for Hawaiian Telecom Services Company, Inc., and 7454 for Wavecom Solutions Corp.

STIR/SHAKEN Implementation

While Hawaiian Telecom relies on the non-IP exception for the TDM portion of its network, Hawaiian Telecom is still considered a voice service provider with a STIR/SHAKEN implementation obligation acting as a wholesale provider and serving end-users.

Hawaiian Telecom will comply fully with all conditions set forth in the FCC's orders, rules, and policies regarding the implementation of the STIR/SHAKEN framework for intermediate providers, including the First Call Authentication Report and Order and Second Call Authentication Report and Order,¹ as it can also be considered a non-gateway intermediate provider with a STIR/SHAKEN obligation in some instances.

For both of its roles, Hawaiian Telecom is subject to the continuing extension provided in 47 C.F.R. § 64.6304(d) for non-IP networks and therefore is exempt from the requirements of § 64.6301 for the TDM portions of its network. 47 C.F.R. § 64.6304(d). Hawaiian Telecom complies with § 64.6303 through its participation in the ATIS Non-IP Call Authentication Task Force, which is working in the industry to develop a non-internet Protocol caller identification authentication solution. 47 C.F.R. § 64.6303.

Hawaiian Telecom has completed the process of implementing STIR/SHAKEN in the IP portions of its network through use of the TNS Call Guardian Authentication Hub. This is a managed end-to-end call authentication solution that fully satisfies the FCC's STIR/SHAKEN requirements. It provides a standardized approach to call authentication and verification (STIR – RFC 8224, RFC 8225, RFC 8226 and SHAKEN – ATIS-1000074-E, ATIS-1000080, ATIS-1000082).

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that Hawaiian Telecom has implemented to detect and prevent illegal robocalls from originating on its network as of February 1, 2024. Hawaiian Telecom is not a significant source of illegal robocalls at this time and has tailored its robocall mitigation practices to address the areas most at risk of originating illegal robocalls. The measures described below explain how Hawaiian Telecom mitigates and addresses the risk it experiences. Hawaiian Telecom will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should Hawaiian Telecom determine that changes are appropriate, its practices may differ from those described below.

Customer Due Diligence

¹ *Call Authentication Trust Anchor; Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, FCC 20-42 (rel. Mar. 31, 2020); *Call Authentication Trust Anchor*, WC Docket Nos. 17-97, Second Report and Order, FCC 20-136 (rel. Oct. 1, 2020).

- Hawaiian Telcom conducts a comprehensive due diligence and credit review before establishing a contractual relationship with customers, including any upstream carrier customers. Hawaiian Telcom's Security Team will review information about new and renewing customers including, but not limited to type of business, state and country of incorporation as contracts are entered into or renewed. The Security Team will identify customers it believes warrant further investigation based on factors that indicate they may be capable of originating illegal robocalls, such as having been subject to a traceback request or previous robocall enforcement action. This review will be aided by external sources and internet searches as are useful in the process. If the investigation raises a concern, the Security Team, in cooperation with Hawaiian Telcom's account team, will discuss the concerns with the customer and take steps to ensure the customer is aware of and will abide by the restrictions. The Security Team will monitor these customers on a "watch list" to determine if additional actions are necessary. Customers who do not engage in problematic practices after a period of time will be removed from the watch list.
- Hawaiian Telcom monitors all of its services for violations of its Acceptable Use Policy (AUP), including excessive use.
- Hawaiian Telcom will terminate or suspend service to customers with a history of non-compliance with its contractual obligations, including provisions relating to acceptable use of the service.

Measures to Prevent or Avoid Exchanging Illegal Robocalls

Hawaiian Telcom will prevent the origination of illegal robocalls on its voice network and assist with tracing and stopping illegal robocalls originating on other service providers networks. This is achieved through:

- **Contractual Provisions** – Hawaiian Telcom's tariffs, service agreements, and Acceptable Use Policy prohibit unlawful uses of service and provide for suspension and/or disconnection for violations of these provisions. Subscribers have an obligation not to use the services for any unlawful purpose, not to engage in any fraudulent uses, and to cooperate with Hawaiian Telcom in mitigating unlawful activities. In addition, Hawaiian Telcom's contracts require subscribers to cooperate with the Company to investigate reports of unlawful activity, including cooperating with traceback requests.
- **Robocall Monitoring Procedures.** Hawaiian Telcom uses TNS Call Guardian analytics technologies and services to monitor traffic on its network and identify potentially unlawful call origination. TNS provides reputation monitoring of originating numbers of Hawaiian Telcom customers and enables Hawaiian Telcom to identify changes in the reputation score and suspicious activity. Hawaiian Telcom has developed a process to investigate incidents identified by this process. The investigation will include determination if the calls are originating on the Hawaiian Telcom network (or, for example, are the result of third parties spoofing numbers associated with Hawaiian Telcom subscribers or have been the subject of previous traceback requests), and will conduct appropriate follow-up with subscribers to remedy any problems or mitigate the

situation. If effective action is not taken, HTI can suspend and/or terminate service to the subscriber.

- **Preventing Calling Line ID (CLID) “Spoofing.”** Hawaiian Telcom does not assist or enable its customers to “spoof” telephone numbers on the services it provides. To the extent a subscriber has customer premises equipment that enable spoofing, Hawaiian Telcom has no involvement in such activity. However, spoofing in violation of the Truth in Caller ID Act violates Hawaiian Telcom’s terms of service and is grounds for suspension and/or termination of service.
- If necessary, Hawaiian Telcom has the ability to block calls from certain providers whose filings do not appear in the Robocall Mitigation Database.

Responding to Traceback Requests

- Hawaiian Telcom will follow the relevant ITG Best Practices to facilitate its response to traceback requests, including specifically:
 - **Dedicated Point of Contact** – Hawaiian Telcom has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual. Although to date Hawaiian Telcom has not received any traceback requests, it has provided the ITG with the contact information and business hours for those individuals according to the ITG’s procedures.
 - **Ongoing Coordination** – Hawaiian Telcom will coordinate with the ITG and other voice service providers in relation to instances of suspicious traffic, including exchanging information related to such traffic and ad hoc follow-up as appropriate.
 - **Prompt Investigation and Response** – Upon receiving a traceback request from the FCC, law enforcement, or the ITG, Hawaiian Telcom will fully respond to the traceback request within 24 hours of receipt of the request. In the event Hawaiian Telcom is unable to respond to a traceback request, it will provide sufficient information in the traceback portal as to why it is unable to respond.
 - **Privacy of Traceback Investigations** – Hawaiian Telcom will not share information about traceback investigations, except with the ITG, with other providers involved in the traceback investigation, or when pursuant to a valid legal process.
- Hawaiian Telcom maintains current and correct information about its upstream carrier customers so that it can provide accurate responses to traceback requests.
- Hawaiian Telcom will periodically review records of traceback requests to identify customers that are the subject of a pattern of traceback inquiries. Hawaiian Telcom will determine an appropriate action to take on a case-specific basis, which may include directing the customer to remedy the problem and, if effective action is not taken, temporary suspension of the customer and/or termination of the customer’s service.

- Hawaiian Telcom will maintain records of any traceback request it receives and the customer involved in the request.

Cooperation with State and Federal Regulators

Hawaiian Telcom will cooperate with state and federal regulators to prevent any and all illegal robocalls. Specifically, Hawaiian Telcom will:

- Respond to requests for information about illegal robocalls;
- Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities; and
- Implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.