

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN

Pursuant to 47 C.F.R. § 64.6305, **ENA Healthcare Services, LLC (“ENAH” or “the Company”)** submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. This plan describes its implementation of STIR/SHAKEN and the practices and procedures currently in place to mitigate illegal robocalls. ENAH may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time in order to respond to changes in its business, its capabilities and its needs.

STIR/SHAKEN Implementation

ENAH complies fully with the conditions set forth in the FCC’s 2020 Report and Order mandating the implementation of the STIR/SHAKEN framework, as well as with the Commission’s related subsequent rulings, and the FCC’s rules and policies generally.

ENAH has implemented STIR/SHAKEN through the use of the MetaSphere QCall service. 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).

ENAH fully supports STIR/SHAKEN in the IP Portions of its network and this traffic is fully attested. Voice traffic is exchanged to the Public Switched Telephone Network (PSTN) via IP in all areas, except where the regional ILEC refuses to participate.

Robocall Mitigation

This Robocall Mitigation Plan (“Plan”) describes the measures the Company implements to prevent and detect illegal robocalls on its network. The Company will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described.

Risk Assessment

ENAH offers a variety of voice calling services. Its voice customers generally do not originate high volume calls and ENAH has not received information suggesting that robocalls are originated on its network. Therefore, ENAH does not consider its network at high risk of originating illegal robocalls. However, even before the FCC’s robocall mitigation measures were required, ENAH carefully scrutinized “high volume call origination” customers to protect its network capacity and cost exposure.

Know Your Customer & Know Your Upstream Provider (collectively, “KYC”)

ENAH carefully reviews all prospective and renewing voice service customers to help ensure their intended use of the services is legitimate and in compliance with FCC robocalling requirements.

- ENAH completes a KYC form for each new and renewing voice customer (attached herein as Exhibit A). Additional/ongoing reviews are conducted if certain business or service changes occur (e.g., new high-risk activity such as auto-dialing or high volume calling).
- ENAH carefully reviews and validates the collected information. ENAH may perform an enhanced review if a customer is in a higher-risk category or if there are questions as to the validity of collected information. Enhanced reviews may include additional questioning to further understand the customer’s intended use of the service, and whether they have been the subject of any prior enforcements or suspected illegal activity related to the same or similar services.
- ENAH has an enforceable acceptable use policy in place. ENAH also has practices in place designed to detect and mitigate fraudulent traffic on its network, such as toll fraud.

Traffic Analytics

In addition to its KYC process, ENAH performs traffic analytics to monitor for unusual or suspicious activity.

- If ENAH has a reasonable basis to believe that a customer is originating illegal robocalls, and/or if a customer is the subject of a traceback request, ENAH will require the customer to cooperate fully and remedy the problem. If effective action is not taken, ENAH’s contracts allow for suspension and/or termination of the service, and the Company may reject/block fraudulent activity.
- ENAH uses Equinix’s TeleLink for end user originated analytics, and RouteTrust for intermediate provider transit traffic call analytics.
- Regarding traffic towards our end users, ENAH uses the Call Guardian service from TNS/Metaswitch for reputation-based call screening and blocking. In addition, our calling name service includes reputation information provided by Neustar in the caller name field presented to our end users (US only).

24-Hour Response to Traceback Requests

ENAH has a dedicated point of contact for addressing traceback requests, as identified in the database, and backup personnel to that individual.

- ENAH is committed to responding fully, within 24 hours, to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and will cooperate with such entities in investigating and stopping illegal robocallers that use its service to originate, carry, or process illegal robocalls.
- If a pattern of questionable activity is detected, ENAH will require its customer to remedy the problem, and if effective action is not taken, ENAH's contracts allow service to the customer to be suspended and/or terminated.

Cooperation with State and Federal Regulators

ENAH will cooperate with state and federal regulators to address illegal robocalls. ENAH will:

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

ENAH provides call authentication, labeling, and screening services to its end users. The Company uses a variety of analytic tools to identify suspicious originating, transiting, or terminating voice traffic. ENAH is committed to protecting our network and customers, and to helping identify bad actors in the call path.

Sincerely,

DocuSigned by:

D8QFDCBD4D814F3...
Gabriela Torresani
Associate General Counsel

EXHIBIT A

Know Your Customer Form

The FCC in the US and the CRTC in Canada have implemented regulations aimed at preventing unauthorized or fraudulent use of voice services and ensuring the integrity of the communications network. Compliance with these rules is crucial for the Company to maintain the trust of our customers and follow regulatory guidelines.

Customer Identity & Contact Information

Full Legal Business Name (“Customer”)	
Physical Address of Business Customers must provide a physical address. This cannot be a virtual address, shared office without a dedicated suite/floor, PO box, mail forwarding service, hosted server location, etc.	
Company Website address	
Compliance Contact - Name, Email, Phone number	
Technical Contact - Name, Email, Phone number	
State/Province/Country of Business Incorporation	
Year of Incorporation	
Employer Identification Number US (EIN) or CAN (BN), Tax ID, or other business ID that is publicly available.	

Nature of Customer’s Business & Calling Activity

Does your business (or do your customers) generate auto-dialed traffic?	
Does your business (or do your customers) engage in telemarketing or “consent to call” collection practices?	
Has your business been subject to any prior enforcements or been suspected of or found in violation of any illegal calling activity? If so, please describe.	
Will the services purchased be resold or used to enable other businesses to initiate or receive communications?	

Certification

The undersigned certifies that he/she is an authorized representative of Customer, and that Customer has knowledge the laws prohibiting the generation and transmission of illegal, harassing or otherwise unwanted voice calls. The undersigned also confirms that Customer complies with these laws and consents to disclose all relevant details if questions arise regarding potential violations of these laws.

The undersigned affirms and certifies that all information and answers to questions herein are complete, true, and correct to the best of signatory’s knowledge and belief.

The undersigned represents and warrants that he/she has full capacity and authority to sign this Certification on behalf of Customer.

Name	
Title	
Signature	
Date	