



Powered by Nord Security

Robocall Mitigation Plan **Saily, Inc.**

Saily, Inc. ("**Saily**") submits this Robocall Mitigation Plan in compliance with 47 CFR § 64.6305(d).

Description of Services

Saily resells domestic voice service to travelers visiting the United States. Specifically, Saily procures wholesale network access from an upstream provider and delivers retail services to its customers under Saily's own brand through eSIM-based provisioning. Saily does not have a STIR/SHAKEN implementation obligation because Saily lacks control of the infrastructure necessary to implement STIR/SHAKEN.

Reasonable Steps to avoid originating illegal robocall traffic

Saily maintains contractual terms with its users that are intended to prevent the origination of illegal calls. For example, the Saily Terms of Service ("**Terms**"):

- (i) permit Saily to intervene in cases of excessive usage,
- (ii) prohibit use of the services for fraudulent, unlawful, or abusive communications, and
- (iii) require users to comply with applicable law. Saily may suspend the services without notice for any breach of the Terms, upon suspicion of fraud or unlawful access to the services, and to prevent network damage caused by a user.

Know-Your-Customer Practices

Saily vets its subscribers by collecting their names, email addresses and payment data. Saily's onboarded KYC vendor processes data (name, surname, sex, personal ID document number, personal ID number (if assigned), date of birth, personal ID document expiry date, photograph(s) of the personal ID document, date, IP address, and manner of personal identification) related to the user verification process and issues this data on demand through an API-based on webhook requests.

Saily applies the following measures to verify identity and detect fraudulent sign-ups:

- (i) KYC identity verification via an onboarded KYC vendor, including verification of the user's personal ID document, photograph, and method of identification;
- (ii) (verification of credit/debit card payments prior to completion of purchase;
- (iii) verification of the payor's email address and device information through Saily's and its payment processor's fraud management tools;
- (iv) logging of IP addresses associated with sign-ups and transactions;
- (v) detection of repeat free-trial abuse by the same individual, device, or email address, with immediate termination of access; and
- (vi) the right to request proof of identity and to suspend services where fraudulent or unlawful access is suspected.



Powered by Nord Security

Additionally, the Terms contain language to prevent anyone other than the original account holder from using the services. For example, the Terms require users to deactivate their Saily eSIM before sharing their device with another person and to inform Saily if their device has been lost or stolen so that Saily may deactivate the Services.

Know Your Upstream Provider Practices

Saily's upstream provider is Telroaming Advanced Communication Solution Ltd. (doing business as '**Webbing**'), and Saily has verified that Webbing is registered in the Robocall Mitigation Database.

Webbing has existing contractual arrangements with U.S. mobile network operations that facilitate the provision of voice service to Saily. Webbing has confirmed that each of these MNOs is listed in the Robocall Mitigation Database.

Description of Analytics to Block Illegal Traffic

Saily does not use analytics to identify and block illegal traffic.

Commitment to Respond to Traceback Requests

Saily is committed to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.