

Robocall Mitigation Plan

Threshold Communications, LLC (“Threshold” or “Company”) serves as the voice service provider in the call chain, with a full STIR/SHAKEN implementation that serves end-users to provide voice-based services (“Service” or “Services”)

The Company has not been prohibited from filing a certification in the Robocall Mitigation Database.

Threshold, nor any of our executives or principals, has a history of enforcement actions for illegal robocalls, TCPA, TSR, or related state law violations.

Threshold uses the affirmative and effective measures detailed below to prevent the origination or transit of illegal robocalls:

Know Your Customer

We follow caller ID authentication best practices to vet caller identity and operational legitimacy for new and existing customers, as described by the NANC Call Authentication Trust Anchor Working Group.

The following information is collected from our customers during the standard onboarding process:

- Name.
- Federal taxpayer ID.
- Physical and mailing addresses.
- Contact telephone numbers.
- Email addresses of principals and controlling persons of the entity.
- Any person with a majority ownership interest in the customer.
- Staff who are responsible for compliance with TCPA, TSR, and other such laws.

For those involved in telemarketing, we additionally collect the customer’s Do Not Call Registry subscription account number, Universal Service Fund registration number, a copy of their FCC 499, and Section 214 International Authority (if applicable).

Our process includes collecting and reviewing entity-identifying information to confirm that we have an authenticated relationship with the customer. We use this authenticated information to

determine whether the customer is subject to any enforcement actions that restrict the types of calls they may make, for example, if they have been banned from initiating telemarketing calls.

Threshold, when possible, validates that the entity has a legitimate right to use the calling numbers it asserts. We use this information to support the attestation level we assign to calls that we originate for that customer.

Our contractual provisions with customers prohibit them from initiating illegal robocalls. If we find a customer initiating suspicious robocalls, we warn them to stop. If such traffic continues, we will then terminate their service.

Traceback

Threshold responds to all traceback requests from the Commission, law enforcement, and the registered traceback consortium, and cooperates with these entities to investigate and stop any illegal robocallers who use our service to originate calls.

Robocall Mitigation Program

Call analytics software provided by Sansay is used to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls. This software provides detailed reporting to identify suspected illegal robocalls. The system blocks and alerts us if we process outbound calls whereby the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list.

Threshold Communications also maintains a detailed history of CDR records. These records can be pulled into our log management, analytics, and data visualization platform for further investigation.

As permitted by FCC 47 CFR 64.1200(k), we block a call when an originating number is malformed, unallocated, on a Do Not Originate list, and/or analytics software or prior activity indicates the call is likely an illegal robocall. As required by this federal regulation, we provide our customers information on how to opt out of call blocking (47 CFR 64.1200(k)(3)(iii)).

The same mitigation steps are applied to all inbound and outbound calls, regardless of our role in the call chain.

Threshold immediately investigates any identified suspicious calls to determine if the caller was attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely

unlawful, we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, we will terminate their service.

There is also a periodic manual review of blocked calls to ensure previous call blocking was proper and act accordingly if, after investigation, it's found the blocking was erroneous, as required by the FCC

Fourth Report and Order in the matter of "Advanced Methods to Target and Eliminate Unlawful Robocalls" (FCC 20-187).

Threshold is prepared to block calls or terminate service from any customer or source if directed by the FCC.

Threshold relies on our voice origination carriers to comply with all common-sense and FCC requirements and accept traffic only from providers with an RMD filing, as required by 47 CFR 64.6305(d).

STIR/SHAKEN

Threshold's STIR/SHAKEN solution is supplied by Sansay. The company is registered with the STI-PA using OCN 563J and holds our own STIR/SHAKEN certificate, issued by the Sansay Certification Authority (STICA), which is used to authenticate calls originating from our system.

Chandler Hume

Threshold Communications, LLC

CTO

Chandler@thresholdcommunications.com

206-812-6200