

Robocall Mitigation Plan

Business Information

Barcks Corp
2235 W 77th Street
Hialeah, FL 33016

Contact Information

Juan Robaina
President 954-217-1193
jrobaina@barcks.net

This robocall mitigation plan is for BARCKS CORP, with headquarters at 2235 W 77th Street Hialeah, FL 33016

Purpose

The FCC requires that facilities-based VSPs certify in the Robocall Mitigation Database that they have implemented a Robocall Mitigation Plan ("RMP") to ensure that they are not originating illegal robocalls.

The FCC requires that VSPs develop a RMP that:

- details the reasonable steps taken to avoid originating illegal robocalls;
- demonstrates a commitment to respond to traceback requests to cooperate with investigators and stopping illegal robocalls; and
- is filed in the Robocall Mitigation Database.

The FCC states that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Barcks Corp is dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. This document outlines Barcks Corp's RMP.

We perform the following roles in the call chain:

- A voice service provider with a STIR/SHAKEN implementation obligation serving end-users

Barcks Corp has not been prohibited from filing a certification in the Robocall Mitigation Database.

Barcks Corp does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations.

Barcks Corp uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls.

Know Your Customer

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

This process includes the collection and review of 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 type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

We also validate, when possible, that the entity has a legitimate right to use its asserted calling numbers. 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, then we terminate their service.

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with Barcks Corp in which we transmit, originate, and/or terminate calls on behalf of the subscriber.

Barcks Corp's KYC program involves obtaining specific subscriber information at the time of sale (i.e. for paid subscriptions), including physical business location and contact person(s).

Acceptable Use Policy ("AUP")

Barcks Corp maintains an AUP, in the form of requirements and restrictions in its Terms of Service, that subscribers must accept before being permitted to use Barcks Corp's services. Among other things, the AUP prohibits:

- violating any applicable law;
- providing false or deceptive information intended to impersonate another; and
- using Barcks Corp's service to engage in, or in connection with, fraudulent activities.

Barcks Corp's contractual terms with subscribers specify that Barcks Corp may take action up to suspension or termination of service for violation of the AUP.

Know Your Upstream Provider

We have a vetting and review process for upstream providers, that is, providers that send us voice traffic that we terminate.

We confirm that the upstream provider has a certification in the Robocall Mitigation Database. We will not accept voice traffic from an provider who has not filed in the Robocall Mitigation Database.

We require that upstream providers have a reasonable robocall mitigation plan, including a vetting process for their customers and upstream providers, and use call analytics to identify suspicious traffic.

Our contractual provisions with upstream providers prohibit them from sending us illegal robocalls. If we find that an upstream provider is sending us suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

Traceback

We respond within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. We cooperate fully with such entities in investigating and stopping any illegal robocallers that use our service to originate, carry, or process illegal robocalls.

Barcks Corp follows Industry Traceback Group ("ITG")-recommended industry standard practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, we believe that Barcks Corp has devoted sufficient resources to provide prompt and complete resources to traceback requests and will continue to do so.

Robocall Mitigation Program

Barcks Corp is dedicated to stopping illegal calls from originating in Barcks Corp's network and monitoring the calls coming into its network, in accordance with FCC regulations.

Barcks Corp certifies that it will cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Barcks Corp certifies that all voice traffic which originates on its network is subject to this robocall mitigation program.

Barcks Corp certifies that as part of its robocall mitigation efforts it is taking these specific reasonable steps to avoid originating illegal robocall traffic:

1. Ongoing review of our customer's calling numbers to confirm that all customer's numbers are consistent with the use cases as described in ATIS-1000089.v0021
2. Periodic reviews of Call Detail Records for suspicious behavior
3. We immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.

Plan updates: This Robocall Mitigation Plan will evolve to respond to the constantly changing practices and techniques that are used to detect and prevent illegal robocalling. Barcks Corp will continue to monitor industry best practices and improve its internal processes to ensure that this Robocall Mitigation Plan is current. In the event of any material change to this Robocall Mitigation Plan, Barcks Corp will submit such update to the FCC's Robocall Mitigation Database.

STIR/SHAKEN

We have registered with the STI-PA using OCN 993J. We have our own STIR/SHAKEN certificate issued by the TransNexus Certification Authority (STI-CA) that we use when authenticating calls we originate. We have implemented a STIR/SHAKEN solution supplied by TransNexus.

We have implemented Out-of-Band SHAKEN for calls that rely on non-IP technology using a STIR/SHAKEN solution supplied by TransNexus.

Monitoring

Barcks Corp works to detect a calling pattern consistent with illegal robocalls and works with its underlying carriers in their similar efforts. If such a call is detected by us or our carriers we will identify the party that is using our services to originate those calls and will take appropriate action. Taking appropriate action may include, but is not limited to, conducting a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls using our services.

No third-parties are involved in deploying Barcks Corp's robocall mitigation analytics.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, our risk prevention team is alerted which follows the defined procedures on investigating such subscribers.

The procedures established include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends (e.g., spikes in call volume);
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.

Telephone Number Authorization

A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify an outbound caller for screening purposes that is uniquely associated with the subscriber. Barcks Corp directly manages the TNs used by its subscribers. Barcks Corp tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Barcks Corp's assignment of the TN to its subscriber.

Barcks Corp does not support customer updates to calling line identity.

When originating a call, Barcks Corp checks the calling party number against Barcks Corp's inventory and will not allow calls unless the calling party number is a TN that has been properly validated.

Blocking

Barcks Corp will implement Do Not Originate requests it receives from the ITG. Barcks Corp has mechanisms to automatically block suspicious calls using internal analytics. If Barcks Corp's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Barcks Corp will take appropriate action which may include suspending or terminating the subscriber's use of Barcks Corp's network. Barcks Corp will cooperate with investigative bodies and law enforcement (including the state attorney general's office), in each case, with applicable authority and a valid request, as well as the FCC and/or the ITG and will document requests and actions taken in response thereto.

Do Not Originate (DNO) Protection

Our company has implemented **Do Not Originate (DNO)** protection using technology supplied by **TransNexus**. This solution enables us to identify and block outbound call attempts that originate from telephone numbers that are not authorized to place calls, including invalid, unallocated, unassigned, or inbound-only numbers. The TransNexus DNO system continuously monitors signaling activity and enforces call authentication and policy controls to prevent unauthorized origination of traffic from our network. This proactive safeguard helps mitigate spoofing, reduce illegal robocall activity, and ensure compliance with FCC robocall mitigation requirements.