

Bark Technologies, Inc.
Robocall Mitigation Plan
(March 1, 2026)

Introduction

This Robocall Mitigation Plan (RMP) details the reasonable steps and actions taken by Bark Technologies, Inc. ("Bark") to mitigate and eliminate illegal robocalling. Bark has an ongoing commitment to identify and help alleviate illegal robocalling by pre-qualifying prospective customers, monitoring existing customers for traffic patterns indicative of prohibited robocalls, and working with other providers and regulatory agencies in combatting fraudulent voice activity.

Bark provides retail voice and data services. All calls that originate on its network are subject to a robocall mitigation program. All telecom services rely extensively on Bark's underlying provider(s) for STIR/SHAKEN implementation and other robocall mitigation efforts.

The Company is not a foreign voice service provider.

The Company does not sell services to international call originators using North American Numbering Plan Numbers.

Compliance History

The Company (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has not been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

No prior RMD certification has been removed by the Commission. The Company has not been prohibited from filing in the Robocall Mitigation Database by the Commission.

The person within the Company responsible for addressing all robocall mitigation-related issues is:

Name: Trent Scovell

Title: Chief Operating Officer

Department: Executive

Telephone Number: (678) 503-7755

Email Address: trent@bark.us

STIR/SHAKEN Implementation

All telecom services are provided on a resale-only basis. The Company is, therefore, exempt from the requirement to implement STIR/SHAKEN because, as a reseller, it lacks control over the network infrastructure necessary to implement STIR/SHAKEN. See First Caller ID Authentication Report and Order, 35 FCC Rcd at 3241, para. 40; 47 CFR Section 64.6304(b). As further detailed herein, the Company has taken steps appropriate for, and required of, a reseller to mitigate robocalling.

The Company uses a third-party vendor/underlying carrier to sign its calls and does not have its own token. Bark does not allow its customers to spoof CallerID, so any outgoing CallerID can easily be traced back to Bark's customer.

The Company does not use a third-party call analytics vendor (not including analytics provided by its underlying service provider(s)). The Company relies on its underlying carrier partners' (T-Mobile's) network-level traffic monitoring, call analytics, spoof detection, and automated blocking tools to identify and mitigate suspicious or potentially unlawful calling patterns.

Traceback Requests

The Company commits, in connection with its underlying service provider, to respond fully and in a timely manner 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.

If a traceback exposes an existing customer as the source of fraudulent robocalls, or as having transmitted fraudulent robocalls, a demand for an explanation and verification of mitigation of the traffic is issued to the customer. If the fraudulent traffic is not remediated, Bark initiates blocking of all traffic from the offending customer.

The Company's point of contact to handle traceback requests is:

Name: Trent Scovell

Title: Chief Operating Officer

Department: Executive

Telephone Number: (678) 503-7755

Email Address: trent@bark.us

Know Your Underlying Provider

Bark has a master service agreement with its underlying service provider and has received confirmation that it will continue to sign calls originated by Bark and will abide by the FCC's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice services to Bark.

Bark and its upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Know Your Customer

Based on the nature of the service which the Company offers to individual cellular subscribers, the risk for robocalling, erroneous telemarketing, and other possible nefarious activity is *extremely* low. Since the service is provisioned on a cellular device, which in most cases is not compatible with auto dialers (and/or other tools which could generate High Volume Short Duration (HVSD) calling) the risk for any form of robocalling is extremely and inherently low.

Nevertheless, Bark has implemented Know Your Customer policies when onboarding new or renewing customers to ensure that such customers do not or are not likely to engage in any prohibited conduct. The Company requires agreements to be signed by an authorized person.

Bark will not activate clients that provide anonymous information or where data mismatches are found. Additionally, Bark is implementing strict Acceptable Use Policies (AUP) prohibiting the act of fraudulent voice activity as a condition of doing business with Bark. Bark investigates prospective customers' information, which may include information such as email address, mobile phone number, service location, IP address validation, CAPTCHA challenges, and mobile app attestation.

Ongoing Robocall Mitigation

Bark, in connection with its underlying service provider, monitors and examines customer traffic to detect suspicious call activity and/or calling patterns. When Bark and/or its underlying providers detect network usage patterns consistent with illegal robocalls or suspect illegal robocalling is taking place, Bark will immediately seek to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action. The actions taken may include, but are not limited to, initiating a traceback investigation; verifying that the originating customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's name; block (or initiate blocking) the party's ability to originate, terminate, or route calls on the network; and/or providing notice to law enforcement authorities.

As part of its plan to mitigate and prevent any originating robocalls, Bark, in connection with its underlying service provider, is committed to early identification and investigation of possible robocalling conditions. Among other things, Bark watches for higher-than-normal subscriber traffic volume, including large bursts of traffic in small timeframes or spikes in usage. Bark also monitors for originating calls of short duration and low call completion percentages and originating calls with sequential “called to” number dialing patterns.

Updating Bark’s RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(d)(5), (e)(5) and (f)(5), Bark will update its submission in the RMD within 10 business days of any change to the applicable information it must provide and update in the RMD.

The Company’s RMP continues to develop as the Company and the industry gain expertise and deploy new robocall mitigation strategies and will be supplemented in future updates.