

AD HOC LABS ROBOCALL MITIGATION PLAN

I. Background

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers to, among other things, file certifications and robocall mitigation plans in the FCC’s Robocall Mitigation Database (“RMD”). 47 CFR § 64.6305; see also *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18 (Mar. 17, 2023) (“*Sixth Caller ID Authentication Report and Order*”).

The FCC requires that all voice service providers certify in the Commission’s RMD whether they have implemented the STIR/SHAKEN authentication framework, and that all of the calls that it originates, carries or processes are subject to a robocall mitigation program consistent with the Commission’s rules. The provider’s mitigation plan “shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment 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.” 47 C.F.R. § 64.6305(a)(2).

Despite imposing a general duty to mitigate “robocalls,” the Commission’s codified rules do not define “robocall.”¹ The TRACED Act defines “robocall violation” as “a violation of subsection (b) or (e) of section 227 of the Communications Act of 1934.” TRACED Act § 11(d), Pub. L. No. 116-105, 133 Stat. 3274 (2019); *id.* at § 13(d)(f)(3) (defining a “suspected unlawful robocall” as a “call that the Commission or a voice service provider reasonably believes was made in violation of subsection (b) or (e) of section 227 of the Communications Act of 1934.” Thus, Ad Hoc Labs’ training and mitigation efforts focus on potentially unlawful calls that violate either (a) 47 U.S.C. § 227(b) (governing non-emergency calls initiated with a prerecorded or artificial voice or an automatic telephone dialing system, as that term has been interpreted by the Supreme Court in *Facebook, Inc. v. Duguid*, 592 U.S. 395 (2001)) or (b) 47 U.S.C. 227(e), or the Truth in Caller ID Act, which prohibits people from causing “any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value,” absent an applicable exemption.

The FCC’s rules contemplate that the provider’s plan should describe how it “complies with its obligation to know its customers pursuant to § 64.1200(n)(4), any procedures in place to know its

¹ The Commission’s TCPA-related regulations, 47 C.F.R. § 64.1200, use the undefined term “illegal traffic,” 47 C.F.R. § 64.1200((k)-(m)), while its STIR/SHAKEN-related regulations define the FCC’s public-facing Robocall Mitigation Database, but not the “robocalls” that are to be mitigated. 47 C.F.R. § 64.6300. Thus, neither of the regulations that bear directly on the project of robocall mitigation expressly define “robocall.” Cf. *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Report and Order and Further Notice of Proposed Rule Making, 32 FCC Rcd. 9706, 9725 56 (Nov. 17, 2017) (declining to define “illegal robocall,” and acknowledging that “the record shows confusion regarding how the proposed definition of ‘illegal robocall’ should apply to the call blocking rules.”); *In re Core Communications, Inc., et al. Tariff F.C.C. No. 3*, WC Docket No. 21-191, Order, 36 FCC Rcd. 9997, 9999 (June 23, 2021) (In a related context, stating that the “Commission defines a robocall as a call made using an automatic telephone dialing system or an artificial or prerecorded voice.”) (citing 47 U.S.C. § 227(b)(1); 47 CFR § 64.1200(a)). Ad Hoc Labs therefore focuses on the two types of unlawful calls—227(b) and 227(e) of the TCPA—that Congress expressly addressed.

upstream providers, and the analytics system(s) it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s).” 47 C.F.R. § 64.6305(d)(1)(ii). The Commission has acknowledged, however, that, “we do not currently require providers other than gateway providers to engage in ‘know-your-upstream-provider’ procedures, but if they have put such procedures in place, they must be documented in their robocall mitigation plan,” and that “we do not specifically require providers to use call analytics.” *Sixth Caller ID Authentication Report and Order* 40 & n.155-56.

The Commission has explained that a robocall-mitigation program is “sufficient if it includes detailed practices that can reasonably be expected to significantly reduce” the provider’s origination or carriage of illegal robocalls, and the voice service provider complies with the practices described in its plan. *Sixth Caller ID Authentication Report and Order* 31. Ad Hoc Labs is dedicated to developing and taking reasonable steps, consistent with FCC regulations and its “[Best Practices](#)” guidance. This document outlines Ad Hoc Labs’ robocall mitigation plan.

II. Ad Hoc Labs’ Know Your Customer (“KYC”) Standards

Ad Hoc Labs is a mobile application and information service provider that, among other functions, facilitates its end-users’ communications via their underlying wireless service devices. Ad Hoc Labs takes substantial measures to ensure the identity of its customers and prevent the use of the service by customers for the origination of robocalls.

Prior to initiating service, all Ad Hoc Labs end users must have their accounts directly linked to (1) a verified phone number or (2) a verified Google, Apple, or Facebook account via a single sign-on process. All customers who create an account must agree to Terms of Service, whereupon they agree to and understand the terms that apply to the use of Ad Hoc Labs’ services. The Terms of Service require customers to agree to provide and maintain true, accurate, current, and complete information about the customer as required by the registration form, and to update the information as necessary. In addition, customers must either be the owner of the voice and/or data plan for the mobile device on which Ad Hoc Labs’ services will be used or have authorization and consent from the device owner to use the services on the mobile device

Ad Hoc Labs’ app is exclusively available through the Apple and Google Play stores, providing unique advantages for the verification of subscriber information. Specifically, in order to make use of either the Apple or Google Play stores, users must have established accounts with Apple and Google, which requires the provision of a payment method for users who make purchases, and an address associated with such payment method. While some users choose to pay for the app with a valid credit card outside the App Store, the payment method is validated by our payment processor, Stripe, at the time of sign-up to pay for a subscription. Regardless, users are still only able to access the app through one of the above App Stores. Of course, Apple and Google maintain much more information on their users than simply a payment method, like device-related information, IP addresses used to connect to their stores and services, and many other data points allowing for identifying individuals who make purchases or download apps.

In addition, outside of direct KYC, Ad Hoc Labs’ network detection systems include manual and automated systems for detecting fraud, particularly during the sign-up and early usage phases, such as detecting bots and non-human actors, ensuring previously deactivated users can’t rejoin and verifying a user’s geolocation is outside of known high-fraud areas and otherwise does not

exhibit suspicious patterns.

III. Ad Hoc Labs' Acceptable Use Policy

The Terms of Service prohibits use of the service for illegal purposes, which prohibited uses include transmission of unsolicited or unauthorized advertising, promotional materials, commercial activities and/or sales, "junk mail," "spam," "chain letters," "pyramid schemes," "contests," "sweepstakes," or any other form of solicitation. Ad Hoc Labs also reserves the right to restrict use of the service where such use may expose Ad Hoc Labs to liability of any type. The Terms of Service further prohibit the use of the services to violate any applicable local, state, national, or international law, any regulations having the force of law, caller ID spoofing, use for high volume or multi-person calling purposes, and attempts to mislead others as to the identity of the sender or origin of any communication made using the service. Customers who become aware of a prohibited use of the service must immediately notify Ad Hoc Labs and provide reasonable assistance in any resulting investigation.

Ad Hoc Labs reserves certain rights through its Terms of Service to ensure that the service is not used for prohibited purposes. For example, Ad Hoc Labs is permitted to monitor the use of the service to ensure compliance with applicable laws and to ensure customer compliance with the Terms of Service. Ad Hoc Labs may discontinue (temporarily or permanently) the service with or without notice to the customer and may block access to the service. Ad Hoc Labs reserves the right to refer to appropriate law enforcement any suspected fraudulent, abusive, or illegal activity through the service.

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

Ad Hoc Labs lacks the necessary facilities and control over the network infrastructure necessary to implement STIR/SHAKEN, and therefore does not have a STIR/SHAKEN implementation obligation. *See Sixth Caller ID Authentication Report and Order* 36 & n. 137; *id.* 45 & n.170. Outbound call initiation occurs via a manual user interface; no volume dialing, robo-dialing, or other automation is possible.

V. Proactive Network Monitoring

Consistent with its Terms of Service, Ad Hoc Labs systems monitor for users/accounts that exhibit abusive behavior (e.g., call velocity, unique destination count, short-duration call volume, inbound/outbound imbalance, unique dialing patterns, account sharing, etc.) and if any accounts are deemed abusive, they are automatically blocked by Ad Hoc Labs and the accounts are suspended.

Ad Hoc Labs partners with Cloudmark, a Proofpoint company that aggregates threat intelligence across billions of messages and calls globally, to enhance real-time detection and blocking of spam, fraudulent, and illegal robocall traffic on its network.

Inbound voice communication is screened against a list of known robocallers and blocked upon matching against a commercially available list that is updated in real time.

VI. Commitment to Timely Traceback Responses and Cooperation

Ad Hoc Labs commits to respond fully and in a timely manner, 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, carry, or process illegal robocalls. Ad Hoc Labs will dedicate sufficient resources to provide timely and complete responses to such requests, and will investigate suspicious activity found by its monitoring systems or reported to it by appropriate parties and take appropriate action.

VII. Enforcement Matters

The filing entity has not, at any time in the prior two years, 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.