

Robocall Mitigation Plan

AUDIAN, INC.

I. Background

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers, like Audian, Inc. (“Audian”), 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, by February 26, 2024, 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.” 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, Audian’s training and mitigation efforts focus, as they must, 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

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. Audian is dedicated to developing and taking reasonable steps, consistent with FCC regulations and its “Best Practices” guidance. This document outlines Audian’s robocall mitigation plan.

II. Audian’s Know Your Customer (“KYC”) Standards

Audian is a Managed Services (“MSP”) and voice service provider that focuses its business and operations on the small and medium-sized business segment of the voice services communications market in its local service territory. As part of its customer-onboarding process, Audian undertakes various commercially reasonable precautions to verify a given customer’s identity as part of entering into a formal written agreement, and ordinarily meets personally with prospective customers as part of the sales and onboarding process, such that it essentially always “knows” its customers in the traditional, human sense of the word.

Among other steps, Audian investigates the prospective customer’s background, such as checking for a company website, the amount of time the business has been open, and other indications of a legal, operating business. Audian routinely deploys its equipment and services at the customer’s location and therefore confirms their domestic business nature and is privy to their usage practices. As of this filing, none of Audian’s business customers are call centers or other high-call-volume operations likely to generate illegal robocalls; none of its customers use any dialers or other software capable of generating high call volumes or prerecorded/artificial voice calls, and it only serves retail end users, not wholesale carrier customers. Its end users also cannot manipulate their Caller ID to display a phone number that Audian has not assigned them, such that they should be incapable of making a call that violates either 227(b) or 227(e).

Among other data points collected and, as appropriate, verified, as part of those KYC processes, Audian gathers the following customer-identifying facts and circumstances, which it typically verifies when it visits its customers’ premises to install and deploy its equipment and services:

- Customer business name,
- Physical business location,
- Contact person(s), and

- Email address.

Audian does not serve wholesale carrier customers. If it does, however, Audian acknowledges that its verification practices would be expanded to include confirming a carrier customer's reported status in the FCC's Form 499 Filer database of registered carriers, and the Commission's Robocall Mitigation Database, along with a completed USF exemption certificate.

III. Audian's Acceptable Use Policy

As part of its customer-onboarding process, Audian's customers contractually agree to various terms and conditions, including a commitment to comply with Audian's Acceptable Use Policy (AUP). Among other things, Audian's AUP prohibits:

- Using the Services to engage in any activities that are illegal, abusive, false, fraudulent, deceptive or misleading, or any activity that exploits, harms, or threatens to harm children.
- Engaging in any unsolicited advertising, marketing, or other unlawful activities using the Services, including, without limitation, any activities that violate laws applicable to advertising, electronic communications, and telemarketing, including, but not limited to, Section 5 of the FTC Act (15 U.S.C. § 45), the CAN-SPAM Act (15 U.S.C. §§ 7701-7713), the Telemarketing Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108), the Federal Trade Commission Telemarketing Sales Rule (16 C.F.R. § 310 et seq.), the Telephone Consumer Protection Act (47 U.S.C. §§ 227), the Federal Communications Commission regulations (47 C.F.R. 64.1200 et seq.) and orders implementing the Telephone Consumer Protection Act, and all federal and state Do Not Call and calling-time restriction laws and regulations.
- Using Audian's Services in any way that fails to conform to any applicable industry guidelines and standards, including, without limitation, the CTIA Messaging Principles and Best Practices, Short Code Registry Best Practices, and Short Code Monitoring Handbook.
- Creating a false identity, forged email address or header, phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or phone call, including failing to comply with the Truth in Caller ID Act.

Audian's contracts with its customers stipulate that Audian is authorized to suspend and/or terminate all Services in the event of an AUP violation. Audian has never received any complaints or tracebacks about its customers' traffic, so, as of this filing, has never had to invoke its AUP.

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

Audian has fully implemented the STIR/SKAKEN authentication framework across its entire network and all calls for which it serves as the originating carrier are compliant with 47 C.F.R. Sec. 64.6301(a)(1)-(2).

All customer phone numbers are either assigned directly by Audian or ported into Audian's carrier partner networks as a condition of providing services, and Audian's end users can only use telephone numbers to which they have subscribed from Audian, such that Audian has a documented, verified relationship between the originating end user and their telephone number(s) used to originate all of their outbound calls. Further, Audian does not allow its customers to change their Caller ID number displayed on their calls, such that their Caller ID accurately reflects their assigned telephone number(s). Should that change and customers could use as a caller ID any number not assigned by Audian, or ported into Audian's network by the end user, Audian will document the end user's right to use the associated phone number(s) from the unaffiliated provider. As such, by design, Audian's end users should be incapable of even making telephone calls from spoofed caller IDs.

V. Proactive Network Monitoring

Audian has various monitoring and reporting systems in place directly and via its upstream carriers to analyze traffic on its network for potentially suspicious traffic patterns that are likely to be associated with illegal robocalls or other potentially unlawful usage. For example, Audian's SIP trunking provider and monitoring systems are capable of assessing traffic based on various criteria, including data relating to call frequency per line, short-duration calls, answer-seizure ratios, and other anomalous call patterns.

Audian also uses software provided by TransNexus to monitor its outbound voice traffic in real time to prevent the origination of illegal robocalls. The software provides detailed reporting identifying suspected illegal robocalls and alerts us any call are originated where the calling number is invalid, unallocated, on a Do Not Originate list, in the FCC consumer complaint database or has a poor reputation. We immediately investigate any identified calls to determine if the caller was attempting to originate unlawful robocalls. If we determine that the caller was attempting to originate unlawful robocalls, then we either warn them to stop or terminate their service as appropriate.

If those systems and/or Audian detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, Audian will take prompt action to identify the party that is using its network to carry these calls and take appropriate action. Once suspected unlawful traffic is discovered, Audian will block any further traffic from being carried associated with the Media IP address of that suspicious traffic. In the event Audian discovers any suspicious traffic that is not demonstrably unlawful, Audian will complete its investigation, and their service can be temporally suspended while that process is completed depending on the severity of the complaint.

VI. Commitment to Timely Traceback Responses and Cooperation

Audian 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



 (844) 737-7374  www.audian.com
 11232 120th Ave NE #206, Kirkland, WA 98033

cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate, carry, or process illegal robocalls. Audian 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.



Simplicity. Speed. Service.