



Voyce
8200 Greensboro Drive, Ste 820
McLean, VA 22102

I. Background

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers, like Voyce (“Voyce”), 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.¹ 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); *id.* at § 64.6305(c)(2) (parallel rule for non-gateway intermediate providers’ “carrying or processing illegal robocall traffic”).

Despite imposing a general duty to mitigate “robocalls,” the Commission’s codified rules do not define “robocall.”² The TRACED Act defines “robocall violation” as “a violation of

¹ See <https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf> (WCB Jan. 25, 2024 Public Notice).

² 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

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, Voyce’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.

By design, Voyce’s services are provisioned in a manner to prevent its end users from violating either of these subsections of the TCPA. First, its system is incapable of generating the telephone numbers its end users may use Voyce’s voice services to call. Like traditional phone service, Voyce’s end users must supply and choose the phone numbers it calls with Voyce’s service. Second, Voyce’s end users must make live-agent calls; Voyce’s services are not compatible with using prerecorded or artificial voice calls (any more than a traditional desk or home phone would be). As such, 47 U.S.C. § 227(b) violations simply should not, and in our experience do not, occur via Voyce’s services. And, third, Voyce’s end users can only use caller IDs that they have been assigned by Voyce as their outbound caller ID, such that, absent some hacking event, which would violate Voyce’s AUP, Voyce’s end users can’t manipulate their caller ID. Thus, by design, Voyce’s end users are likewise prevented from using Voyce’s services to violate 47 U.S.C. § 227(e).

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) [for originating voice service providers], 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); *see also* 47 C.F.R. § 64.6305(f)(2)(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

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)). Voyce therefore focuses on the two types of unlawful calls—227(b) and 227(e) of the TCPA—that Congress expressly addressed.

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. As illustrated in this plan, Voyce is dedicated to developing and taking reasonable steps, consistent with FCC regulations and its “[Best Practices](#)” guidance. This document outlines Voyce’s robocall mitigation plan.

Know Your Customer

Voyce has established a thorough pre-screening process before onboarding new clients to ensure all “Know Your Customer”/KYC documents are reviewed and approved by third party legal counsel. The KYC process includes validating the following: their legal name and address, contact name and information for both legal compliance and billing. FCC Registration Number (FRN), FCC 499 Filer ID, and tax exemption status. Voyce also confirms a certification is filed in the Robocall Mitigation Database, checks industry and financial references, the number of years in business, number of ITG tracebacks received, as well as a series of questions related to the origination of traffic and the traffic profile.

If the prospect is not in compliance, Voyce will decline to move forward.

Blockings Tools

Voyce utilizes a variety of network tools to combat illegal robocalls. Specifically, and pursuant to rules adopted by the Commission in FCC 17-151, Voyce blocks calls from phone numbers on Do-Not-Originate (“DNO”) list from SOMOS. Voyce has the ability of blocking calls from non-LERG ANIs, invalid and wireless numbers.

Voyce utilizes RoboGuard to block media IPs reported as being associated to scam calls, FCC or CLEC complaints.

If a call comes from a “Neighboring” number, meaning the NPA-NXX is the same on both the ANI and DNIS, such call will be blocked.

Caller ID Blocking Tool (CDI) – The system monitors CDI profiles for low Answer Seizure Ratio (ASR), low Average Length of Call (ALOC), high Short Duration Percentage (SDP), if an ANI reaches the set threshold, the ANI will be blocked. In addition, an internal team monitors customer traffic profiles daily for traffic profile changes and will contact a customer via email or a phone call to validate the traffic profile change and demand the removal of any suspected illegal calls. If not corrected in a timely manner, the route is suspended. When route(s) are suspended, all attempted call(s) will be returned back to the originator with the appropriate SIP response code and the call(s) are terminated before they reach a Voyce vendor or the Public Switched Telephone Network (PSTN).

Contract Termination – Voyce typically has contractual rights that allow it to terminate customers that violate relevant law, including violations of the Telephone Consumer Protection Act. When appropriate, Voyce enforces these rights. Subject to applicable laws that may prevent it from doing so, Voyce may also terminate accounts if it discovers that any of the entities or individuals associated with a customer account have been named by the FCC or the FTC as an illegal robocaller or have failed to respond to traceback requests.

Traceback Requests

Voyce 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. Voyce 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.

If a client is the originator of the traceback, they are given a warning to remove the source. If an additional traceback is received, the client is terminated immediately.

STIR/SHAKEN (S/S)

Voyce has implemented STIR/SHAKEN to all egress/outbound traffic. Traffic received with a S/S token will be passed and will not be altered. Voyce is actively blocking traffic received without a S/S token with no exception.

For Inbound Traffic, VoyceAdmins offers a suite of features beneficial for businesses needing to adhere to Robocall Mitigation Database rules, focusing on artificial intelligence (AI) to enhance call management and security.

Key features include:

AI Assistance and Call Filtering: AI is utilized for managing and filtering calls, which can help distinguish between legitimate and spam calls, supporting robocall mitigation efforts.

Call Recording and Security: The platform emphasizes secure operations and the privacy of user data, alongside offering call recording capabilities.

Customizable Call Management: Features such as selective call forwarding, call screening, and the ability to block unwanted callers are provided, leveraging APIs and caller ID for effective call identification.

Enhanced Customer Service: By using AI to support caller interactions and reducing wait times, VoyceAdmins aims to improve customer service and support.

These features highlight VoyceAdmins' potential to help businesses manage calls efficiently and securely, in line with Robocall Mitigation Database requirements.

VoyceAdmins leverages IVR (Interactive Voice Response) technology as a core part of its feature set. IVR systems are instrumental in managing incoming calls by directing callers through menu options, which can be tailored to meet various needs. This functionality is crucial for Robocall Mitigation Database compliance, as it allows businesses to efficiently filter and manage calls, ensuring only legitimate interactions proceed. IVR systems like those provided by VoyceAdmins leverages VoiceAlerts Data which can play a significant role in identifying, managing, and mitigating unwanted robocalls as per FCC regulations.

Voyce discloses that it received a notice from the Social Security Administration dated February 22, 2023 in which the Administration alleged that SSA-related scam traversed Voyce's network. Voyce complied with the Notice's requirements and provided all requested documentation. Voyce never heard from the Administration in response and assumes the matter is closed.