

VOICESHOT, LLC
ROBOCALL MITIGATION PLAN – MARCH 2025

I. Background

The Federal Communications Commission (“FCC” or “Commission”) required that all voice service providers certify, by June 30, 2021, in the Commission’s [Robocall Mitigation Database](#) whether they have implemented STIR/SHAKEN or, if subject to an applicable extension, that they have documented and instituted a robocall-mitigation plan to help combat the origination of illegal robocalls on their networks.¹ The Commission has explained that a robocall-mitigation program is sufficient if the detailed practices in the plan can “reasonably be expected to significantly reduce the origination of illegal robocalls” and the voice service provider complies with the practices it describes in its filings.

VoiceShot is dedicated to stopping illegal calls from originating on its network, and this document outlines VoiceShot’s current Robocall Mitigation plan.

II. Commitment to Traceback Cooperation

VoiceShot commits to timely cooperating with and responding to Traceback requests from the FCC Enforcement Bureau, ITG (or any successor entity designated by the FCC), trace-forward investigations, and other valid law enforcement and government demands, subpoenas, and other valid legal processes. VoiceShot will dedicate sufficient resources to provide prompt and complete responses to such requests. VoiceShot will investigate suspicious activity found by its monitoring systems or reported to it by consumers or third parties and take appropriate action.

VoiceShot has adopted the following additional internal procedures to carry out its commitment to cooperate with Traceback requests and to take appropriate remedial actions when warranted:

- David Carriveau, VoiceShot’s Director of Voice Services, has been designated the responsible officer and will coordinate the handling of all Traceback requests that are received.
 - Mr. Carriveau is overseen by VoiceShot’s CEO, John Wright. Mr. Wright, together with VoiceShot’s Chairman Mark Jennings, are the principals of VoiceShot. VoiceShot is affiliated with TrueDialog, Inc., a text messaging service platform for enterprise customers.
- When a traceback request is received, VoiceShot will email the customer a list of questions necessary to properly investigate the scope of the Traceback request and if the calls are legitimate or not.
- VoiceShot will also promptly call the relevant customer to inform them of the Traceback request, and that VoiceShot has sent the customer an email requesting specific information related to the investigation.

¹ See <https://docs.fcc.gov/public/attachments/DA-21-454A1.pdf>.

- **If the customer does not respond within 24 hours, VoiceShot will suspend the account** – without limiting other actions VoiceShot may take.
- VoiceShot will separately perform an audit of the subject account, and suspend or terminate the account if deemed to be sending illegal content or calls in violation of VoiceShot’s Terms of Service.
- VoiceShot’s goal is to comply with all Traceback requests within 24 hours if commercially reasonable, and sooner when practicable.

III. VoiceShot’s Know Your Customer (“KYC”) Standards

VoiceShot is a voice and text service provider that focuses its operations on the government, non-profit and business customer segment of the communications market. As part of its customer-onboarding process, VoiceShot undertakes various commercially reasonable precautions to verify a given customer’s identity as part of entering into a formal written agreement.

During the initial prospective-customer screening process, VoiceShot collects the following customer-identifying information when possible:

- Customer entity or business name,
- Customer email,
- Customer physical address,
- Customer telephone numbers,
- Federal tax ID number (if applicable),
- State of incorporation (if applicable), and
- Contact person(s).

Once obtaining this information, VoiceShot support and sales staff will attempt to contact all prospective customers during the enrollment process for further vetting. VoiceShot then requires the prospective customer to verify all caller IDs to be used through VoiceShot’s service through a verification process that entails VoiceShot placing an outbound call with a pin code to each telephone number, which the prospective customer must then enter to verify the telephone number.

IV. VoiceShot’s Acceptable Use Policy

As part of its customer-onboarding process, all of VoiceShot’s customers contractually agree to various terms and conditions, including a commitment to comply with VoiceShot’s Terms of Service. Among other things, the Terms of Service provide that:

- Subscriber is fully and solely responsible to be aware of, understand, and comply with all of the rules and regulations applicable to Subscriber's use of VoiceShot Service including but not limited to Federal Trade Commission rules and regulations, Federal Communication Commission rules and regulations, National Do Not Call Registry rules

and regulations and individual state Do Not Call rules and any applicable individual state or local regulations, CAN-SPAM, the Controlling the Assault of Non-Solicited Pornography and Marketing Act, along with any other federal, state, or local laws that may be applicable to Subscribers use of VoiceShot Service. Subscriber agrees not to violate these, or any other federal, state, or local law and represents and warrants that Subscribers use of VoiceShot will not cause VoiceShot to violate these or other similar laws.

- Subscriber shall at all times comply with all applicable laws, statutes, regulations, rules, ordinances, codes, and standards, including but not limited to the Telephone Consumer Protection Act of 1991 and any amendments thereto, at 47 U.S.C. § 227, the Federal Communications Commission implementing regulations, at 47 CFR § 64.1200 et seq., the Federal Trade Commission's Telemarketing Sales Rule at 16 CFR Part 310 and any amendments and any similar laws, CAN-SPAM, the Controlling the Assault of Non-Solicited Pornography and Marketing Act, federal and state laws proscribing unfair or deceptive acts and practices, federal and state telemarketing laws, and laws governing wages, hours, desegregation, employment discrimination, employment of minors, health, safety and personal information and any other similar laws. Subscriber agrees not to violate these, or any other applicable federal, state, or local anti-solicitation laws, and represents and warrants that its use of VoiceShot Service will not cause VoiceShot to violate these or other similar laws.
- Subscriber understands that the Federal Trade Commission Telemarketing Sales Rule prohibits the transmission of pre-recorded phone calls that are part of a plan, program or campaign which is conducted to induce the purchase of goods or services or charitable contributions. The Federal Trade Commission Telemarketing Sales Rule provides that calls may be permissible provided calls are placed only to consumers who have provided their prior expressed signed written consent to receive such calls. Use of VoiceShot Service for the delivery or transmission of pre-recorded phone calls that are part of a plan, program or campaign which is conducted to induce the purchase of goods or services or charitable contributions not in compliance with applicable law is strictly prohibited. Notwithstanding the language contained in this paragraph calls initiated and placed by the Subscriber specifically to consumers who have provided the Subscriber with their prior expressed signed written consent to receive such calls as provided by the Federal Trade Commission Telemarketing Sales Rule at 16 CFR Part 310 and any amendments thereof shall not be deemed prohibited. Subscriber understands that compliance with federal, state and local law is solely the responsibility of the Subscriber.
- Subscriber understands and agrees that if Subscribers use of VoiceShot Service includes initiating or receiving telephone calls to or from customers or donors then Subscriber shall comply with all applicable federal, state and local laws including but not limited to

laws pertaining to telemarketing.

VoiceShot's contracts with its customers stipulate that VoiceShot is authorized to suspend and/or terminate all Services in the event of a customer using the Service in violation of these requirements. In addition, VoiceShot has an entire webpage persistently linked on its website that provides compliance resources regarding the TCPA, the TSR, the DNC Registry, and Commission guidance regarding the same. VoiceShot encourages any potential customer that is unsure of their legal compliance obligations to consult with an attorney, and reminds them of the potential consequences of violating these consumer protection laws.

V. Telephone Number Authorization and STIR-SHAKEN Capabilities

VoiceShot resells TDM-based outbound one-way broadcast services to its end users. Given VoiceShot's status as a TDM reseller, VoiceShot is not subject to STIR/SKAKEN implementation requirements, and it otherwise lacks control over the network infrastructure necessary to implement STIR/SKAKEN. As noted above, however, VoiceShot's end users can only use telephone numbers which they have verified are assigned to them, such that VoiceShot has a documented, verified relationship between the originating end user and their telephone number(s) used to originate their calls.

VI. Proactive Network Monitoring and Fraud Prevention

VoiceShot has various monitoring, fraud prevention and reporting systems in place 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, VoiceShot disallows prospective customer enrollment from foreign countries, or if a potential customer attempts to register with an email address from a free email service (such as Gmail), VoiceShot will not permit the customer onboarding process to continue unless VoiceShot personnel can speak with the potential customer to conduct further vetting. VoiceShot further uses advanced credit card fraud prevention practices to stop transactions from occurring before outbound traffic can be initiated by customers. VoiceShot also uses automated processes to detect patterns consistent with illegal robocalls or other likely scams. More specifically, in addition to its internal processes and analytics used to detect anomalous traffic patterns, VoiceShot's underlying voice services are provided using Lumen's TDM-based voice services. As part of VoiceShot's relationship with Lumen, Lumen will provide additional call-analytics reporting to VoiceShot based on various calling metrics. Pursuant to FCC Rule 64.6305(d)(2)(ii), VoiceShot states that Lumen is the only third party who provides call analytics services utilized by VoiceShot.

VoiceShot has also enabled additional features that allow call recipients to place themselves on the calling party's internal DNC list.

VII. Additional Information Required By *Sixth 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.² 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).³

VoiceShot notes that, by design, its services are provisioned to significantly curtail end users' ability to spoof their telephone numbers. VoiceShot's end users can only use caller IDs that they have individually verified on a number-by-number basis, through the process described above, as their outbound caller ID, such that, absent some hacking event, which would violate VoiceShot's AUP, VoiceShot's end users cannot manipulate their caller ID. Thus, by design, VoiceShot's end users are prevented from using VoiceShot'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), 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. That said, VoiceShot directs the Commission to its KYC standards detailed above.

² See <https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf> (WCB Jan. 25, 2024 Public Notice).

³ 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, VoiceShot's training and mitigation efforts focus, consistent with the TRACED Act, 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.