

EXHIBIT TO CERTIFICATION OF IOVOX INC. FOR ROBOCALL MITIGATION DATABASE

Updated: February 10, 2026

As part of iovox, Inc.'s ("iovox") submission to the Robocall Mitigation Database, pursuant to Section 64.6305 of the Commission's rules,¹ this document outlines (1) the reasonable steps iovox has taken to avoid carrying or processing illegal robocall traffic; (2) iovox's commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium; and (3) iovox's commitment to cooperate with such entities in investigating and stopping any illegal robocallers that use the gateway provider's service to carry or process calls. This Robocall Mitigation Plan ("RMP") serves to provide the Commission with specific details regarding iovox's mitigation strategy.

Robocall Mitigation Plan

For the services iovox provides, it is a Non-Gateway Intermediate Provider, receiving calls from, and delivering calls to, tier 1 network providers. iovox is not a voice service provider because it does not originate or terminate any voice traffic to end users. iovox does not have an obligation to fully implement the STIR/SHAKEN Framework because it does not receive any voice traffic directly from any originating voice service provider.² All voice traffic received and delivered by iovox is received from and delivered to other intermediate providers.

This RMP applies to iovox's calling platforms and provides information on iovox's policies procedures regarding steps taken to avoid carrying illegal robocall traffic, responding to traceback requests, and cooperating during the investigation of illegal robocall traffic:

1. Efforts to Avoid Carrying or Processing Illegal Robocalls

iovox has made investments to combat carrying or processing illegal robocalls. Though iovox primarily only allows for inbound calling, iovox provides the following solutions on the iovox network to help minimize the impact of illegal or unwanted robocalls to customers, in the rare instance such a call is even possible to complete:

- **Know Your Customer:** Consistent with the FCC's Caller ID Authentication Best Practices No. 1³ and 47 C.F.R. § 64.1200(n)(3), iovox vets "the identity of retail and wholesale subscribers by: (i) approving an application for service; (ii) provisioning of network

¹ 47 C.F.R. § 64.6305.

² See 47 C.F.R. § 64.6302(d) (requiring non-gateway intermediate providers to authenticate "all calls it receives directly from an originating provider and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call"); *In the Matter of Call Authentication Trust Anchor*, Sixth Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 17-97, FCC 23-18, ¶ 17 (2023) (explaining that "the *first intermediate provider* in the path of an unauthenticated SIP call will now be subject to a mandatory requirement to authenticate the call") (emphasis added).

³ *Wireline Competition Bureau Issues Caller ID Authentication Best Practices*, WC Docket Nos. 17-97 and 20-324, DA 20-1526, at Appendix A (rel. Dec. 22, 2020) ("FCC's Caller ID Authentication Best Practices"), <https://docs.fcc.gov/public/attachments/DA-20-1526A1.pdf>

connectivity; (iii) entering into a contract agreement; or (iv) granting the right-to-use telephone number resources.”⁴ As such, iovox takes “affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic.”⁵ Along these lines, iovox has implemented Know Your Customer (“KYC”) procedures for onboarding new customers. This KYC program includes the following required submissions by prospective customers:

- o Full legal name of the company
- o State or country of incorporation
- o Physical address of primary operations
- o Billing name and address
- o Customer contact name and telephone number
- o Description of the company’s business model
- o Summary of the intended uses of the iovox services

Additionally, prior to the execution of any contract with a prospective customer, iovox will check government information sources to determine if the prospective customer has had any prior ITC traceback requests, as well as FCC/FTC sources to determine if the prospective customer has been identified as a robocaller.

- **Contract Termination:** Voice service customers of iovox are subject to terms and conditions that (1) obligate customers not to use iovox’s services for unlawful purposes; and (2) preserve iovox’s right to terminate customers for violations of the law. iovox’s contracts include terms that prohibit customers from using iovox’s services to transmit calls that violate laws restricting robocalls or other telemarketing calls, including the federal Telephone Consumer Protection Act (“TCPA”), and/or the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”). If found in violation of these rules, iovox’s contract terms allow for suspension and remedy provisions or unilateral termination if the offense remains uncured. Subject to applicable laws that may prevent it from doing so, iovox 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 Federal Trade Commission (“FTC”) as an illegal robocaller or have failed to respond to traceback requests.
- **Know Your Upstream Provider:** The company has policies and procedures in place to ensure that it knows the identities from upstream providers from which iovox accepts voice traffic. For example, iovox maintains an active list of its suppliers that includes business and technical contacts. iovox also maintains a limited set of suppliers and ensures that the supplier is identified in the FCC’s Robocall Mitigation Database. iovox also has the ability to determine whether traffic it receives has been authenticated by its upstream network providers.

⁴ *Id.*

⁵ 47 C.F.R. § 64.1200(n)(3).

- **Network Monitoring:** iovox analyzes and monitors the call traffic that originates on, terminates to, or routes through iovox's voice network. iovox monitors the voice traffic patterns on a twenty-four (24) hour basis to identify behaviors that are consistent with illegal robocalling. iovox has in place anti-fraud processes, including traffic sampling at 15-minute intervals. If traffic exhibits a variance from historic patterns, the system automatically creates an alert for support staff to investigate. Investigation entails examining call detail records to identify anomalies. If a determination is made that the calls are suspicious in nature, iovox will block calls using origin and destination parameters and will remove numbers from service or disable the entire account as needed. If iovox discovers a call pattern consistent with robocalling, iovox reserves the right to take further action to address the issue by working with the originating customer to resolve the problematic traffic, continuing to block the problematic calls, and/or terminating the customer's service contract.
- **Blocking Calls:** In accordance with 47 C.F.R. § 64.1200(k)(2) and (o)(1)-(4), iovox blocks calls purporting to originate from a number on a reasonable Do-Not-Originate ("DNO") list that is associated with North American Numbering Plan numbers. iovox has protocols in place to detect DNO calls and blocks calls that are determined to originate from a DNO number.
- **Network Tools:** Among other network tools, iovox uses the following to combat illegal robocalls:
 - Company developed tools to monitor traffic patterns and detect anomalies
 - Database queries designed to identify anomalous traffic
 - Packet captures to analyze low level network traces
 - Automatic velocity-based spam detection and automated blocking of suspicious traffic sources

iovox does not use any call analytics tools provided by third-party vendors.

2. Responding to Traceback Requests and Cooperating in Investigating and Stopping Illegal Robocallers

iovox is committed to ensuring that its network is not used for the origination, termination, or routing of unwanted or illegal robocalls. iovox commits to respond fully and within 24 hours⁶ to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium, per the Commission's rules, 47 C.F.R. § 64.6305(b)(2) and 47 C.F.R. § 64.1200(n)(1)(ii). iovox will cooperate with these entities in investigating and stopping any illegal robocallers that attempt to use iovox's network to carry or process calls. As part of this commitment, iovox commits to take the necessary steps to effectively mitigate illegal traffic when the company receives actual written notice of such traffic from the

⁶ This 24-hour window applies within business days, per rule 47 C.F.R. § 64.1200(n)(1)(ii) and as clarified by the Commission. See FCC 22-37, at n.211.

FCC through the Enforcement Bureau. iovox will comply with the requirements of the notice, in accordance with the Commission's rules.⁷

To further ensure iovox's network is not utilized for the origination, termination, or routing of unwanted and illegal robocalls, iovox provides the following name, title, department, business address, telephone number, and email address of the individual within iovox that handles robocall mitigation-related issues, as well as responds to traceback inquiries from the FCC, Industry Traceback Consortium, and law enforcement agencies:

Dan Luis, Chief Operations Officer
1 Belvedere Drive, Suite 200
Mill Valley, California, 94941
+1 (888) 408 4128
operations@iovox.com

3. STIR/SHAKEN Compliance

iovox provides call analytics and tracking services to clients. These services are managed by providing Direct Inward Dialing ("DID") services to clients, which are pre-set to terminate at a single (and not dynamic) end-user business location. The only way to implement a successful call on the iovox network, without hacking, is for the DID to receive an inbound call. As the call passes through the iovox network, the correct destination is looked up, and the call is passed through. Due to the nature of this system, it is not possible for robocalls to be initiated from the iovox network.

iovox is reliant on its upstream carrier partners to block any robocall attempts on its DIDs. Despite its reliance on upstream providers, and although iovox does not itself authenticate the caller identification information associated with any of the voice calls that it carries or processes, iovox can determine whether calls entering its network environment are signed or unsigned. The company remains committed to responding to all traceback requests and requirements from relevant bodies, including the Commission, law enforcement, and the Industry Traceback Consortium. In the rare instance a hacker attempts to reverse a call, and therefore, make a robocall possible, iovox has implemented rigorous procedures to mitigate illicit robocalls and unauthorized Caller-ID spoofing, as noted in comments above pertaining to network monitoring and call blocking methodologies.

Ownership and Management

iovox is a wholly-owned, direct subsidiary of iovox Limited. iovox does not have any subsidiaries but currently has one affiliate: Wannaspeak.

Information regarding iovox's management team, including the identity of its officers, is available at: <https://www.iovox.com/about>.

Robocall Mitigation Plan Updates

⁷ See 47 C.F.R. § 64.1200(n)(2), (3), & (5).

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(c)(5) & (d)(5), iovox will update its submission in the Robocall Mitigation Database within 10 business days of any change to the applicable information it must provide in the Robocall Mitigation Database, including its RMP.