

ROAM DIRECT, LLC ROBOCALL MITIGATION PLAN

I. Background

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring non-gateway intermediate service providers, like Roam Direct, LLC (“Roam Direct”), to, among other things, file certifications and robocall mitigation plans in the FCC’s Robocall Mitigation Database (“RMD”). 47 CFR § 64.6305(f); *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 non-gateway intermediate service providers to 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 they carry or process are subject to a robocall mitigation program consistent with the Commission’s rules.¹ 47 CFR § 64.6305(f). The provider’s mitigation plan shall include “reasonable steps the non-gateway intermediate provider has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program,” 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 carry or process calls.” 47 C.F.R. § 64.6305(f)(2).

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 subsection (b) or (e) of section 227 of the Communications Act of 1934.” TRACED Act § 11(d), Pub. L. No. 116-105,

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 pertinent to voice service providers, 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)). Roam Direct therefore focuses on the two types of unlawful calls—227(b) and 227(e) of the TCPA—that Congress expressly addressed.

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, Roam Direct’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 also contemplate that the non-gateway intermediate provider’s plan should describe “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 of such vendor(s).” 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 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 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. This document outlines Roam Direct’s robocall mitigation plan.

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

Roam Direct is a wholesale, intermediate provider that focuses its business and operations on the domestic, wholesale voice services communications market. As part of its customer-onboarding process, Roam Direct undertakes various commercially reasonable precautions to verify a given customer’s identity, including having its customers complete a KYC questionnaire, a USF Exemption Certificate, and a formal written contract.

Among other data points collected and, as appropriate, verified, as part of those processes, Roam Direct gathers the following customer-identifying facts and circumstances:

- Customer business name, including DBAs,
- state of incorporation & license/registration number,
- federal tax ID number,
- physical business location,
- contact person(s), with business phone number, physical headquarters address, and email address(es) (which shall include an email domain with an obvious

- nexus to the business name);
- FCC 499 Filer ID and FRN;
- Robocall Mitigation Database link, indicating STIR/SHAKEN compliance, role in call path, and mitigation plan, as applicable;
- Company ownership information;
- IP address usage history for past 3 years;
- Customer's robocall-related judgments or enforcement action history, if any,
- Customer's status as a cooperative VSP with the ITG,
- Discuss and/or review Customer's KYC policy, RMD plan, and traceback history; and
- Company website, social media and other customer-facing presence;

Roam Direct's verification practices include confirming a carrier customer's reported status in the FCC's Form 499 Filer database, and the Commission's Robocall Mitigation Database to ensure it is facially compliant and consistent with the representations made as part of the onboarding process, and the prospective customer has not been delisted by the FCC. Roam Direct also conducts, as applicable, credit checks and checks references with a prospective customer's other carrier-suppliers and reviews the data provided as part of the KYC onboarding process, including verifying data from publicly accessible internet sources.

Roam Direct only provides services to customers that are incorporated in the United States and complete its KYC questionnaire. Roam Direct cross-checks new customers' IPs against Roam Direct's Media IP-block list. When Roam Direct onboards new customers, Roam Direct's fraud team also checks all new account traffic profiles for the first 24 hours by checking ANIs against databases such as YouMail, RoboGuard, and other internal and commercially available sources.

III. Roam Direct's Acceptable Use Policy

As part of its customer-onboarding process, all of Roam Direct's customers contractually agree to various terms and conditions, including a commitment to comply with Roam Direct's Acceptable Use Policy (AUP). See <https://roam.direct/aup/>. Among other things, this 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.

- 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.

Roam Direct's contracts with its customers stipulate that Roam Direct is authorized to suspend and/or terminate all Services in the event of an AUP violation.

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

Roam Direct is a non-gateway intermediate provider that only contractually agrees to accept traffic that is already STIR/SKAKEN-authenticated before it is handed off to Roam Direct for carriage, and therefore does not have a STIR/SKAKEN implementation obligation. *See Sixth Caller ID Authentication Report and Order* ¶ 20 ("the first intermediate provider in the call path may completely avoid the need to authenticate calls if it implements contractual provisions with its upstream originating providers stating that it will only accept authenticated traffic").

As noted above, Roam Direct provides its intermediate voice services solely to other U.S.-based, domestic, FCC-registered originating and intermediate voice service providers. As such, Roam Direct is not the originating provider capable of authenticating the calling party's relationship with the caller ID ascribed to a call originating by U.S.-based voice service providers. Roam Direct's network is, however, already capable of accepting and accurately transmitting all STIR/SKAKEN-related data it receives in the call path.

V. Proactive Network Monitoring and Analytics

Roam Direct is a non-gateway intermediate provider and therefore does not have a direct relationship with a party that may be originating unlawful robocalls. Accordingly, when Roam Direct suspects it has identified potentially unlawful calling, in addition to taking the steps outlined herein, it may also contact the carrier customer from which it received the traffic at issue to investigate their customer from whom they received the traffic at issue. At the same time, Roam Direct reminds mindful of the Commission's long-standing policy of common carriage and not blocking traffic in a manner that, if prevalent, would threaten the ubiquity and seamlessness of the nation's communications network.

Roam Direct has various monitoring 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, Roam Direct's monitoring systems assess and, as applicable, flag or automatically block, traffic based on various criteria, including traffic reported as likely illegal by YouMail's carrier-reporting services, ASR-based blocking, applying a threshold that no more than 10% of a customer's traffic can have an average call

duration of less than 6 seconds, and declining to carry traffic purporting to originate from telephone numbers on Somos's commercially available DNO lists or other invalid, not-in-service ANIs.

Roam Direct also declines to carry calls in real time via third-party robocall mitigation tools and services. Roam Direct has a fraud department that monitors YouMail statistics and blocks the Media IPs of known bad actors to prevent such traffic from entering Roam Direct's network, regardless of the carrier or phone number that the call(s) comes from. Roam Direct's network also deploys the RoboGuard mitigation service provided by FraudCentral.

If Roam Direct detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, Roam Direct takes prompt action to identify the party that is using its network to carry these calls and take appropriate action.

VI. Commitment to Timely Traceback Responses and Cooperation

Roam Direct 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. Roam Direct 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.