

SIPNEX TELECOM LLC ROBOCALL MITIGATION PLAN

I. Background

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers, like Sipnex Telecom LLC (“SIPNEX”), 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 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

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

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, SIPNEX’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, SIPNEX’s services are primarily 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 SIPNEX’s voice services to call. Like traditional phone service, SIPNEX’s end users must supply and choose the phone numbers it calls with SIPNEX’s service. Second, with one exception, SIPNEX’s end users must make live-agent calls; SIPNEX’s services can only be used with prerecorded or artificial voice calls for informational, political calls after going through additional customer screening, during which the customer must either demonstrate representative form of consent or commit to scrubbing wireless numbers out of its contact list. As such, 47 U.S.C. § 227(b) violations simply should not, and in our experience do not, occur via SIPNEX’s services. And, third, SIPNEX’s end users can only use caller IDs that they have been assigned by SIPNEX as their outbound caller ID, such that, absent some hacking event, which would violate SIPNEX’s AUP, SIPNEX’s end users can’t manipulate their caller ID. Thus, by design, SIPNEX’s end users are likewise prevented from using SIPNEX’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 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, SIPNEX is dedicated to developing and taking reasonable steps. This document outlines SIPNEX’s robocall mitigation plan.

II. SIPNEX's Know Your Customer ("KYC") Standards

SIPNEX is a UCaaS software and voice services provider that focuses on the business end user and domestic voice service provider customer segments of the communications market. This plan describes its KYC practices for each type of customer.

As part of its end user customer-onboarding process, SIPNEX undertakes various commercially reasonable precautions to verify a given customer's identity as part of entering into a formal written agreement, and soliciting information from the prospective customers designed to solicit the customer's acknowledgement and recognition that their use of the services is subject to a robust legal and regulatory regime affecting their outbound calling practices. All prospective customers undergo an onboarding process that is personally conducted by SIPNEX personnel that includes phone calls with the prospective customer. New customers cannot enter into an agreement for SIPNEX's services without going through that personalized onboarding process; i.e., there are no online-only subscribers to SIPNEX's services.

As part of that personally reviewed process, SIPNEX personnel investigate the prospective customer's background, such as checking for valid contact information tied to the company subscribing to the services. Among other data points collected and, as appropriate, verified, the following end user customer-identifying facts and circumstances are gathered:

- Customer business name (legal name and DBAs, if any),
- Company email, phone number, and website domain,
- Company physical business address,
- Company state of incorporation and good-standing status, with proof of incorporation and driver's license of principal/owner/corporate representative,
- Company personnel contact name.

SIPNEX's onboarding process also includes the prospective customer's completion of a detailed new-customer questionnaire that solicits details on the customer's anticipated use cases of the SIPNEX services and the compliance implications of their proposed campaign(s), along with a confirmation that they acknowledge the various legal restrictions and conditions surrounding their use of the SIPNEX platform.

With respect to the small number of domestic carrier customers for which SIPNEX provides intermediate services, SIPNEX solicits and verifies their full corporate information consistent with the end user vetting described above, along with their FCC registration information, 499 filer ID, and their FCC Robocall Mitigation Database filing. These wholesale carrier customers contractually agree, among other things, to sign (or have already received signed) all traffic they hand to SIPNEX pursuant to STIR/SHAKEN, and agree that SIPNEX will decline to carry any unsigned traffic they may attempt to deliver to SIPNEX.

III. SIPNEX's Acceptable Use Policy

As part of its customer-onboarding process, SIPNEX's customers contractually agree to various terms and conditions, and their usage of SIPNEX's services is subject to SIPNEX's Acceptable Use Policy (AUP). Among other things, SIPNEX's contract and AUP prohibit:

- 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 SIPNEX'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.

SIPNEX's contracts with its customers stipulate that SIPNEX is authorized to suspend and/or terminate all Services in the event of a violation of these terms or any other unlawful conduct committed through their use of the services.

IV. STIR-SHAKEN Capabilities and Telephone Number Authorization

SIPNEX has fully implemented the STIR/SHAKEN 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).

As noted above, with respect to its non-gateway intermediate provider services, SIPNEX only contractually agrees to accept traffic that is already STIR/SHAKEN-authenticated before it is handed off to SIPNEX for carriage, and therefore does not have a STIR/SHAKEN implementation obligation with respect to such traffic, but it does transmit all STIR/SHAKEN-authentication data it receives from those carrier customers. *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”).

SIPNEX’s end users are only authorized to use and display as their Caller ID the telephone numbers to which they have subscribed from SIPNEX, such that SIPNEX has a documented, verified relationship between the originating end user and their telephone number(s) used to originate those calls.

V. Proactive Network Monitoring

In addition to the significant manual review of customers’ background and use cases described above, SIPNEX 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. SIPNEX also routinely analyzes message delivery rate data as indicia of potentially suspicious or unwanted traffic, and promptly investigates any such customer’s traffic. Any Traceback requests, subpoenas, carrier complaints or similar events likewise trigger a prompt investigation by the company into that customers’ traffic, and it is SIPNEX’s practice and policy to respond to all tracebacks and similar enforcement authority requests within 24 hours.

With respect to its non-gateway intermediate provider services, SIPNEX does not have a direct relationship with a party that may be originating unlawful robocalls. Accordingly, if SIPNEX 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, SIPNEX remains 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.

In addition to its internal analytics-based mitigation practices and protocols, SIPNEX also uses Somos DNO and FraudCentral.io’s Roboguard robocall-mitigation analytics and call blocking tools.

VI. Commitment to Timely Traceback Responses and Cooperation

SIPNEX 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. SIPNEX 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.