

SIPPHONY LLC
ROBOCALL MITIGATION PLAN

I. Background

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

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 the Commission or a voice service provider reasonably believes was made in 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 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)). Sipphony therefore focuses on the two types of unlawful calls—227(b) and 227(e) of the TCPA—that Congress expressly addressed.

subsection (b) or (e) of section 227 of the Communications Act of 1934.”

Thus, Sipphony’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 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.

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. Sipphony is dedicated to developing and taking reasonable steps. This document outlines Sipphony’s robocall mitigation plan.

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

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

All prospective customers participate in an enrollment process supervised by Sipphony staff. Sipphony investigates the prospective customer’s background, such as checking for a company website, the amount of time the business has been open, and other indications of a legal, operating business. Among other data points collected and, as appropriate, verified, as part of those processes Sipphony gathers the following customer-identifying facts and circumstances:

- Customer business name,

- Company email, phone number, and website domain,
- state or country of incorporation,
- physical business location,
- contact person(s), and
- Federal Tax ID (EIN).

Sipphony then verifies the customer's corporate name and status with the records of the state where the customer's corporate status originated. Sipphony also requires that all individuals associated with a prospective customer's application for service provide Sipphony with copies of their drivers' licenses and/or passports. Sipphony also requires that prospective customers provide copies of their most recent bank statement to confirm their identities.

Sipphony also collects various written details about the prospective customer's intended use case(s) for their Sipphony service, including the nature of their business and campaign, how they ordinarily acquire the numbers they typically call, and, if their proposed use case includes sales calls and/or is not solely live-agent calls, their scrubbing practices vis-à-vis wireless numbers and numbers on the DNC Registry, among other considerations.

III. Sipphony's Acceptable Use Policy

As part of its customer-onboarding process, all of Sipphony's customers contractually agree to various terms and conditions, including a commitment to comply with Sipphony's Acceptable Use Policy (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.
- Using Sipphony'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.

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

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

Sipphony 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).

Sipphony's end users can only use telephone numbers to which they have subscribed from Sipphony or numbers they represent they have been assigned from other carriers. In the latter cases, Sipphony undertakes various testing designed to mitigate spoofing risks, which it has not encountered to date because Sipphony's customers almost universally want to be called back, so using a non-functioning number or number not actually assigned to them would defeat the purpose of receiving any calls back to their number.

V. Proactive Network Monitoring and Analytics

Sipphony has various internal 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, Sipphony's switch provider and monitoring systems can assess traffic based on various criteria, including data relating to short-duration calls, SDP/SDR, answer-seizure ratios, call-failure (404) ratios, and ANI Cardinality Ratio, a measure of uniqueness in the ANI distribution to help identify any suspicious calling patterns. Sipphony uses third-party mitigation tools provided via its underlying switch provider, Sipnav.

Sipphony also employs an automated system that utilizes advanced artificial intelligence language models to analyze transcripts of messages stored or transmitted via the service. This system serves as an additional layer of protection on top of the company's personnel's manual campaign review process, which it undertakes regularly, to identify potential AUP issues. The automated system works by scanning outgoing message transcripts for markers of potential fraud or non-compliance with regulatory standards. If there are any changes in rules or regulations, our team can promptly adjust the prompts for the language model.

If Sipphony detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, Sipphony takes prompt action to identify the party that is using its network to carry these calls and take appropriate action. Once suspected unlawful traffic is discovered, Sipphony blocks any further traffic from being carried associated with the Media IP address of that suspicious traffic.

VI. Commitment to Timely Traceback Responses and Cooperation

Sipphony 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. Sipphony 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.

Supplement Regarding Past Agency Correspondence

As the Commission is aware, the Commission's Enforcement Bureau Attorney Advisor, Daniel Stepanicich, sent Sipphony a warning letter dated January 11, 2023 relating to certain identified traffic. Sipphony responded to the Bureau, via counsel, by letters dated January 13, 2023 and January 25, 2023. Sipphony has not received further correspondence from the Bureau regarding the mitigation actions it took vis-à-vis that correspondence.