

SIPIFY LLC

ROBOCALL MITIGATION PLAN

I. Background

The Federal Communications Commission ("FCC" or "Commission") has adopted rules requiring voice service providers, like Sipify LLC ("Sipify"), 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 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, Sipify'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) [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. Sipify is dedicated to developing and taking reasonable steps. This document outlines Sipify's robocall mitigation plan.

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

Sipify is a wholesale, intermediate provider that focuses its business and operations on the wholesale voice services communications market. As part of its customer-onboarding process, Sipify 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 Sipify gathers the following customer-identifying facts and circumstances:

- Customer business name,
- state or country of incorporation,
- physical business location,
- contact person(s), with business phone number and email address;
- federal tax ID number,
- FCC Filer ID;
- Robocall Mitigation Database filing indicating STIR/SHAKEN compliance; and
- Company website and/or other customer-facing presence;

Sipify's verification practices include confirming a carrier customer's reported status in the FCC's Form 499 Filer database of registered carriers, and, as of June 30, 2021, the Commission's Robocall Mitigation Database. Sipify also conducts, as applicable, credit checks and checks references with a prospective customer's other carrier-suppliers.

As of January 2024, Sipify only provides services to new customers that are incorporated in the United States and complete its Robocall Mitigation form. Sipify

cross-checks new customers' IPs against Sipify's Media IP-block list. When Sipify onboards new customers, Sipify's fraud team also checks all new account traffic profiles for the first 24 hours by checking ANIs against databases such as YouMail and other proprietary and/or commercially available sources.

III. Sipify's Acceptable Use Policy

As part of its customer-onboarding process, all of Sipify's customers contractually agree to various terms and conditions, including a commitment to comply with Sipify's Acceptable Use Policy (AUP). See <https://sipify.com/terms>. 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 Sipify'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.

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

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

Sipify has fully implemented the STIR/SHAKEN authentication framework across its entire network. Sipify's network accepts and accurately transmits all STIR/SHAKEN-related data it receives in the call path, consistent with 47 C.F.R. § 64.6302. As noted

above, Sipify provides its intermediate voice services solely to other registered domestic originating and intermediate voice service providers. As such, Sipify is not the originating provider capable of authenticating the calling party's relationship with the caller ID ascribed to a given call, or to the called party.

V. Proactive Network Monitoring

Sipify 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. Sipify employs multiple internal and third-party robocall mitigation and prevention systems, far exceeding legal requirements. For example, Sipify's monitoring systems assess and, as applicable, flag or automatically block, traffic based on various criteria, including:

(a) Internal Do Not Originate (DNO) Database: Sipify curates its DNO lists from multiple Robocall Mitigation Database (RMD) providers to create a robust defense mechanism. The Sipify DNO Database houses over 22,000 U.S. numbers, enhancing its capability to block unwanted originations;

(b) Do Not Terminate (DNT) Database: Our DNT Database features over 4,000 numbers, further strengthening the network's security by preventing unauthorized terminations;

(c) Wireless ANI Blocking: Sipify prevents wireless ANIs from terminating on its network, unless the originating carrier is a registered wireless provider, from a customer understood not to carry wireless-originated traffic;

(d) NPA-NXX Matching Blocking (Neighbourhood Spoofing): Sipify proactively blocks calls that engage in "Neighbourhood spoofing," thereby automatically preventing such calls from terminating on its network by matching NPA-NXXs of the calling and called parties' telephone numbers;

(e) blocking calls for which the caller ID is not a valid, in-service ANI in the LERG;

(f) RealNumber® DNO System: Sipify takes advantage of SOMOS's RealNumber® DNO RMD System to further augment its capabilities. SOMOS manages an expansive database of over 6 billion Do Not Originate (DNO) numbers, along with an additional 28 million Toll-Free DNO numbers;

(g) FraudCentral VoiceGuard® Technology: Sipify leverages a diverse range of RMD products from FraudCentral, including the renowned VoiceGuard® technology. Sipify employs the VoiceGuard® technology within its network infrastructure to proactively block malicious actors at the source by implementing Media IP blocking. Recognized as one of the most effective methods for thwarting bad actors, VoiceGuard® operates a vast network of over 250,000 honeypots across the U.S., enabling real-time identification and mitigation of threats. In addition to its core functionalities, Sipify also leverages VoiceGuard® for specialized services such as Ringless Voice-mail and ASR

Protection, preventing ringless voice-mails from traversing through the Sipify network and providing robust defenses against DDoS (Distributed Denial of Service) attacks and Toll-Free Pumping schemes; see <https://fraudcentral.io>; which leverages far more robust, sweeping and effective mitigation than traditional ANI-based tools have offered to date; and

(h) using Artificial Intelligence to block calls—typically very short duration calls—likely associated with DDOS attacks.

Sipify also declines to carry calls in real time via third-party mitigation tools and services provided via its underlying switch provider. Sipify has a fraud department that operates around the clock and that monitors YouMail statistics and blocks the Media IPs of known bad actors to prevent such traffic from entering Sipify's network, regardless of the carrier or phone number that the call(s) comes from.

Sipify actively monitors and enforces these and other proprietary practices and policies designed to mitigate the misuse of its network. Since December 2021, when Sipify receives a general (as opposed to government-imposter/facially fraudulent) traceback related to a US-based customer, it requires its carrier customers to investigate and as applicable suspend or terminate their subject downstream customer promptly, and advise Sipify of the actions taken to mitigate the issues raised in the traceback, and to remove similar types of traffic from Sipify's network. If Sipify receives a second traceback within 60 days of the first traceback regarding the same customer and campaign type, the customer is terminated immediately. If Sipify receives a general traceback related to a foreign customer, they are terminated immediately. If Sipify receives notice from the Industry Traceback Group that its customer did not complete their traceback request, they are also suspended or terminated. If Sipify receives knowledge, other than through a traceback, that a customer has allowed illegal traffic onto Sipify's network, Sipify warns its customer that they must immediately remove their underlying customer that generated the traffic.

If Sipify detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, Sipify 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

Sipify 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. Sipify 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.

Footnotes:

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