

SOURCE ONE BUSINESS SERVICES, LLC ROBOCALL MITIGATION PLAN

I. Background

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers, like Source One Business Services, LLC (“Source One”), 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 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,

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)). Source One 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, Source One’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), 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. Source One is dedicated to developing and taking reasonable steps. This document outlines Source One’s robocall mitigation plan.

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

Source One is a voice service provider that focuses its business and operations on the business end-user market and as a recent entrant into domestic reseller segment of the wholesale communications market. As part of its customer-onboarding process, Source One undertakes various commercially reasonable precautions to verify a given customer’s identity as part of entering into a formal written agreement. As part of its customer-onboarding process, Source One undertakes various commercially reasonable precautions to verify a given customer’s identity. Those processes can include reviewing 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 as part of working with the prospective customer to provide the best communications products and services to meet their needs. Source One personnel are always personally involved in onboarding a new customer.

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

- Customer business name,
- state or country of incorporation,
- physical business location,
- contact person(s) and contact information, and,
- for wholesale customers, FCC 499 Filer ID, FCC RMD entry, STIR/SHAKEN status, and exemption certificate.

With respect to its end-user customer base, Source One routinely deploys its services at the customer's location and therefore is privy to their usage practices and personally meets and interacts with its end users personally. Source One provisions all of its end users' devices through which the voice services are used, and none are capable of being used as an autodialer, to deliver prerecorded or artificial voice messages, or spoofing their Caller IDs. Thus, by design, Source One's services have never been and are highly unlikely to be used in a way to generate unlawful robocalls.

With respect to its domestic wholesale services, Source One's verification practices include confirming a carrier customer's reported status in the FCC's Form 499 Filer database of registered carriers, and the Commission's Robocall Mitigation Database to ensure it has a current registration at the time of onboarding. If necessary and appropriate, Source One also conducts credit checks and/or checks references with a prospective customer's other carrier-suppliers.

III. Source One's Acceptable Use Policy

Source One's customers' usage of its services must comply with Source One'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 Source One'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.

Source One's AUP authorizes it to suspend and/or terminate all services in the event of an AUP violation.

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

Source One is a non-facilities-based reseller that lacks the necessary facilities and control over the network infrastructure necessary to implement STIR/SKAKEN, and therefore does not have a STIR/SKAKEN implementation obligation. *See Sixth Caller ID Authentication Report and Order* ¶ 36 & n. 137; *id.* ¶ 45 & n.170. For its wholesale traffic, Source One will only contractually accept traffic that is signed or will be signed by Source One's immediately downstream carrier partner that Source One is reselling, and therefore does not have a direct STIR/SKAKEN implementation for such traffic. *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").

Nevertheless, all of Source One's end users' outbound calls originated via the resold services of its immediately downstream carrier partner and number supplier are authenticated, at the applicable levels, in accordance with STIR/SKAKEN by that carrier partner.

Source One's end user customers can only use telephone numbers to which they have subscribed from or ported into their account with Source One (via its downstream carrier partner), such that Source One has a documented, verified relationship between the originating caller and their telephone number(s) used to originate their calls.

V. Proactive Network Monitoring

Source One has various monitoring and reporting systems available 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. Its monitoring systems generate daily reports with usage data. Source One's internal monitoring systems can assess traffic based on various criteria, such as call attempts, call quantity, average call duration, short-duration calls, answer-seizure ratios, and anomalous volumes of 404, 503 and other call-failure codes.

If Source One detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, Source One takes prompt action to identify the party that is using its network carry or originate these calls and take appropriate action. In the event Source One discovers any suspicious traffic that is not demonstrably unlawful, Source One would investigate the basis for the suspect calls, and the customers' service can be temporally suspended while that process is completed depending on the severity of the complaint.

VI. Commitment to Timely Traceback Responses and Cooperation

Source One 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. Source One 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.