

VOIP Essential Robocall Mitigation Plan

VoIP Essential LLC (“VoIP Essential”), in connection with its provision of voice services, maintains these written policies, practices, and procedures to monitor, review, and analyze call traffic, and to use commercially reasonable efforts to identify, mitigate, and block unlawful Robocalls, or investigate patterns consistent therewith, including, without limitation, the consideration of call duration, call volume, calls per second, and, if available to VoIP Essential, the location of the calls’ origination or U.S. point of entry.

I. Background

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers, like VoIP Essential, 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

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

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, VoIP Essential’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.

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

VoIP Essential is dedicated to developing and taking reasonable steps. This document outlines VoIP Essential's robocall mitigation plan.

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

In furtherance of this commitment, VoIP Essential undertakes the following actions:

Before onboarding a new end user or carrier customer, VoIP Essential will comply with applicable federal law, including 47 C.F.R. § 64.1200(n)(3), and the company's Consent Decree with the State of Indiana, to know its originating end user customers and wholesale customers. To implement that so-called "KYC," or Know Your Customer, duty, VoIP Essential requires all new and renewing wholesale customers to complete a detailed KYC form soliciting their corporate and carrier credentials, including 499 and RMD entry and we request and review prior traceback history. End users are required to fill out the data solicited on the VoIP Essential website: <https://dashboard.voipessential.com/customer/register>.

Responsible company personnel then review each prospective customer's KYC submission, and if and as necessary, consult commercially reasonable and available sources to corroborate the information provided by the prospective customer and to follow-up with the customer to address any questions or concerns raised by the KYC process.

Prospective carrier customers' FCC 499 Filer ID and Robocall Mitigation Database status will be checked at these or any successor URLs established by the Federal Communications Commission for such verification purposes:

<https://apps.fcc.gov/cgb/form499/499a.cfm>

https://fccprod.servicenowservices.com/rmd?id=rmd_listings

Further, a prospective carrier customer's status as an authorized voice service provider will be verified via the then-current Policy Administrator's website, which is currently located at:

<https://authenticate.iconectiv.com/authorized-service-providers-authenticate>

VoIP Essential will likewise maintain in good standing its STIR-SHAKEN compliance with the Policy Administrator and Certificate Authority and authenticate calls in accordance with applicable law and ATIS standards.

III. VOIP ESSENTIAL'S ACCEPTABLE USE POLICY

As part of its customer-onboarding process, VoIP Essential's customers contractually agree to various terms and conditions, including a commitment to comply with AM Comm's Acceptable Use Policy (AUP). Among other things, this AUP prohibits:

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, 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, all federal and state Do Not Call and calling-time restriction laws and regulations, Section 5 of the FTC Act (15 U.S.C. § 45), the CAN-SPAM Act (15 U.S.C. §§ 7701-7713), the Federal Trade Commission Telemarketing Sales Rule (16 C.F.R. § 310 et seq.), and the Telemarketing Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108).

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

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

VoIP Essential 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).

In cases where VoIP Essential's end users use telephone numbers to which they have subscribed from VoIP Essential, VoIP Essential has a documented, verified relationship between the originating end user and their telephone number(s) used to originate their calls. In the cases where a VoIP Essential end user is using numbers secured from a different service provider, VoIP Essential documents the end user's right to use the associated phone number(s) from the unaffiliated provider(s).

For traffic for which VoIP Essential serves as an intermediate provider, VoIP Essential's network is capable of accepting and accurately transmitting all STIR/SHAKEN-related data it receives in the call path.

V. Proactive Network Monitoring

In addition to the foregoing KYC and robocall mitigation practices, VoIP Essential also undertakes various commercially reasonable efforts to identify and mitigate unlawful Robocalls, as defined in the Consent Decree and applicable law. For instance, VoIP Essential:

- Blocks traffic from numbers identified on a commercially available DNO (Do Not Originate) list, currently provided via SOMOS;
- Uses an innovative robocall-mitigation tool, RoboGuard, that employs Media IP-based blocking analytics rather than the traditional, inferior ANI-based blocking provided by other commercially available sources to block all calls from Media IP addresses that the service provider has deemed to be highly likely to be scam, fraudulent, already the subject of tracebacks or FCC cease-and-desist published notices, as well as the target of CLEC complaints.
- Tracks and analyzes periodic (monthly, and/or on an as-needed basis) reports that identify various call criteria, including, without limitation, total minutes of use, calls per second, average call duration, answer seizure ratio (in and out), call-completion ratio, blocked CID and Media IP counts, and SIP code-related data, and then analyzes those reports to identify anomalous traffic patterns that warrant further investigation.

VoIP Essential Personnel who support these business and compliance objectives are an integral part of the company's compliance success. They are expected to read and implement these Policies and Procedures, and to bring any questions or concerns they may have about them to Sean Medhi.

VI. Commitment to Timely Traceback Responses and Cooperation

VoIP Essential 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. VoIP Essential 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 Proceedings

VoIP Essential was a party to a federal court proceeding in which the State of Indiana took issue with its robocall-mitigation practices vis-à-vis wholesale traffic it had received from Startel Communications, notwithstanding the fact that VoIP Essential had never received *any* tracebacks concerning their traffic. VoIP Essential denied all material allegations and settled that matter via a publicly available Consent Decree. See Complaint, *Indiana v. Startel Communications LLC et al*, No. 3:21-cv-00150-RLY-MJD (S.D. Ind. Oct. 14, 2021), ECF No. 1; Answer to Complaint, ECF No. 44; Joint Motion for Entry of Consent Decree and Dismissal, ECF No. 58; Entry Granting Joint Motion for Consent Decree, ECF No. 60.