

DESERTLINK COMMUNICATIONS, LLC ROBOCALL MITIGATION PLAN

I. Background

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

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

Desertlink is a voice service provider that focuses its business and operations on the domestic wholesale voice services communications market, and will soon be expanding its operations to include business end user services.

As part of its wholesale-customer-onboarding process, Desertlink undertakes various commercially reasonable precautions to verify a given customer’s identity, including having its customers complete a USF Exemption Certificate, and enter into a formal written contract. Among other data points collected and, as appropriate, verified, as part of those processes Desertlink gathers the following customer-identifying facts and circumstances:

- Customer business name,
- state of incorporation,
- physical business location,
- contact person(s),

- federal tax ID number,
- FCC Filer ID and FRN,
- STIR/SHAKEN status,
- FCC Robocall Mitigation Database link.

Desertlink'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 the listing is current and active and aligns with Desertlink's conversations during the onboarding process. Desertlink also conducts, as applicable, credit checks and checks references with a prospective customer's other carrier-suppliers, and runs searches on publicly available internet sources to assess whether there has been any adverse press regarding the carrier's traffic.

As part of the contracting process, in addition to agreeing to Desertlink's AUP, discussed below, the carrier customers also agree to authenticate (or have already received authenticated) all traffic they hand to Desertlink pursuant to STIR/SHAKEN, and agree that Desertlink will decline to carry any unsigned traffic they may attempt to deliver to Desertlink. Desertlink does transmit all STIR/SHAKEN data it receives in the call flow.

All prospective end-user customers will participate in an enrollment process supervised by Desertlink staff. Desertlink 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 Desertlink 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).

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

III. Desertlink's Acceptable Use Policy

Desertlink's customers' use of its services are subject to Desertlink'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.
- 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.

Desertlink is authorized to suspend and/or terminate all Services in the event of an AUP violation.

IV. STIR-SHAKEN Capabilities

Desertlink is a non-gateway intermediate provider that only contractually agrees to accept traffic that is already STIR/SKAKEN-authenticated before it is handed off to Desertlink for carriage, and therefore does not have a STIR/SKAKEN implementation obligation with respect to that 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, Desertlink has implemented STIR/SKAKEN into its network and is capable of and will authenticate any calls required to be authenticated that it carries.

As noted above, Desertlink provides its intermediate voice services solely to other U.S.-based, domestic, FCC-registered originating and intermediate voice service providers. As such, Desertlink is not the originating provider capable of authenticating the calling party’s relationship with the caller ID ascribed to a call originating by U.S.-based voice service providers. Nevertheless, Desertlink’s network accepts and accurately transmits all STIR/SKAKEN-related data it receives in the call path, consistent with 47 C.F.R. § 64.6302. When Desertlink expands its offerings to include origination services, all traffic originated by its end user customers will be authenticated at the applicable attestation level for such traffic.

V. Proactive Network Monitoring

Desertlink 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. For example, Desertlink's monitoring systems assess and, as applicable, flag or automatically block, traffic based on various criteria, including (a) blocking calls for which the caller ID is not a valid, in-service ANI in the LERG; (b) blocking calls from any Media IP address associated with a known or reported illegal robocalling entity; and (c) using Artificial Intelligence to block calls—typically very short duration calls—likely associated with DDOS attacks. Desertlink's network also uses the VoiceGuard tool provided by FraudCentral to assist its robocall mitigation efforts.

Desertlink, as an intermediate provider, does not have a direct relationship with a party that may be originating unlawful robocalls. Accordingly, if it suspects it has identified potentially unlawful calling, in addition to taking the steps outlined above, 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, Desertlink 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.

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

Desertlink 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. Desertlink 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.