

D3UC LLC
ROBOCALL MITIGATION PLAN

I. Background

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers, like D3UC LLC (“D3UC”), 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)). D3UC 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, D3UC’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. D3UC is dedicated to developing and taking reasonable steps, consistent with FCC regulations and its “[Best Practices](#)” guidance. This document outlines D3UC’s robocall mitigation plan.

II. D3UC’s Know Your Customer (“KYC”) Standards

D3UC is a voice service provider that focuses its business and operations on the wholesale and business customer segments of the voice services communications market. As part of its customer-onboarding process, D3UC undertakes various commercially reasonable precautions to verify a given customer’s identity as part of entering into a formal written agreement.

First, all prospective D3UC customers participate in a roughly two-hour demonstration of D3UC’s services, platform and customer expectations, during which call D3UC discuss the customers’ intended uses of the network and D3UC’s acceptable usage policy. D3UC also 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 D3UC 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, and exemption certificate.

D3UC'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, D3UC also conducts credit checks and/or checks references with a prospective customer's other carrier-suppliers.

III. D3UC's Fair Use Policy

As part of its customer-onboarding process, all of D3UC's customers contractually agree to various terms and conditions, including a commitment to comply with D3UC's Fair Use Policy (FUP). Among other things, this FUP 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 D3UC'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.

D3UC's contracts with its customers stipulate that D3UC is authorized to suspend and/or terminate all Services in the event of an FUP violation.

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

D3UC has fully implemented the STIR/SKAKEN 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).

D3UC's customers, both retail end user and wholesale, can only use telephone numbers to which they have subscribed from D3UC (via its downstream carrier partner), such that D3UC has a documented, verified relationship between the originating caller and their telephone number(s) used to originate their calls. As such, D3UC can readily confirm the caller ID on any given call with the customer associated with that call, and D3UC's system is designed to prevent unlawful spoofing by customers.

V. Proactive Network Monitoring

D3UC 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. D3UC's internal monitoring systems are capable of assessing traffic based on various criteria. The primary criteria D3UC's network uses to monitor a given customer's call patterns is call quantity, which D3UC's network monitors on an automated basis and is set a level that should be well short of likely suspicious outbound traffic volumes. Should such pattern emerge, the customer cannot make further outbound calls without further interaction with D3UC, and D3UC can also evaluate other call data, such as data relating to short-duration calls, answer-seizure ratios, and anomalous volumes of 404, 503 and other call-failure codes. D3UC does not use any third-party analytics vendors for purposes of its robocall mitigation efforts.

If D3UC detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, D3UC takes prompt action to identify the party that is using its network carry or originate these calls and take appropriate action. In the event D3UC discovers any suspicious traffic that is not demonstrably unlawful, D3UC 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

D3UC 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. D3UC 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.