

DID CENTRAL LLC ROBOCALL MITIGATION PLAN

I. Background

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers, like DID Central LLC (“DID Central”), 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

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

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

DID Central 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, DID Central 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 DID Central 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;

DID Central'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. DID Central also conducts, as applicable, credit checks and checks references with a prospective customer's other carrier-suppliers.

As of January 2022, DID Central only provides services to new customers that are incorporated in the United States and complete its Robocall Mitigation form. DID Central cross-checks new customers' IPs against DID Central's Media IP-block list. When DID Central onboards new customers, DID Central'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. DID Central's Acceptable Use Policy

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

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

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

DID Central has fully implemented the STIR/SKAKEN authentication framework across its entire network. DID Central'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. As noted above, DID Central provides its intermediate voice services solely to other registered domestic originating and intermediate voice service providers. As such, DID Central 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

DID Central 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, DID Central's monitoring systems assess and, as applicable, flag or automatically block, traffic based on various criteria, including:

- (a) matching NPA-NXXs of the calling and called parties' telephone numbers;
- (b) calls with a caller ID of a telephone number associated with a wireless carrier from a customer understood not to carry wireless-originated traffic;
- (c) blocking calls for which the caller ID is not a valid, in-service ANI in the LERG;
- (d) blocking calls purporting to be from a telephone number on Somos' DNO list;
- (e) blocking calls from any Media IP address associated with a known or reported illegal robocalling entity, including Media IP addresses sourced from DID Central's affiliate's proprietary, FraudCentral robocall-mitigation suite of tools; see <https://fraudcentral.io>; which leverages far more robust, sweeping and effective mitigation than traditional ANI-based tools have offered to date; and
- (f) using Artificial Intelligence to block calls—typically very short duration calls—likely associated with DDOS attacks.

DID Central also declines to carry calls in real time via third-party mitigation tools and services provided via its underlying switch provider. DID Central 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 DID Central's network, regardless of the carrier or phone number that the call(s) comes from.

DID Central actively monitors and enforces these and other proprietary practices and policies designed to mitigate the misuse of its network. Since December 2021, when DID Central 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 DID Central of the actions taken to mitigate the issues raised in the traceback, and to remove similar types of traffic from DID Central's network. If DID Central receives a second traceback within 60 days of the first traceback regarding the same customer and campaign type, the customer is terminated immediately. If DID Central receives a general traceback related to a foreign customer, they are terminated immediately. If DID Central receives notice from the Industry Traceback Group that its customer did not complete their traceback request, they are also suspended or terminated. If DID Central receives knowledge, other than through a traceback, that a customer has allowed illegal traffic onto DID Central's network, DID Central warns its customer that they must immediately remove their underlying customer that generated the traffic.

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

DID Central 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. DID Central 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.