

BYTEWORTH LLC ROBOCALL MITIGATION PLAN

I. Background

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

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 the Commission or a voice service provider reasonably believes was made in violation of subsection

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

(b) or (e) of section 227 of the Communications Act of 1934.” Thus, Byteworth’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), 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). 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. Byteworth is dedicated to developing and taking reasonable steps. This document outlines Byteworth’s robocall mitigation plan.

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

Byteworth is a small voice service provider that focuses its business and operations on the small business segment of the voice services communications market. While most of its service offerings are non-regulated information services, it has begun offering some VoIP service offerings to complement its other innovative communications solutions. Byteworth does not allow its users to make calls using artificial, prerecorded or AI-generated voice.

As part of its customer-onboarding process, Byteworth undertakes various commercially reasonable precautions to verify a given customer’s identity as part of enrolling that customer in one or more of its service plans. Byteworth investigates the prospective customer’s background, such as securing individual consumers’ names, addresses, emails, payment information and, if applicable, current phone provider details to implement the porting process associated with moving their telephone number(s) to a Byteworth service plan. For small business customers, Byteworth also solicits company name and legal address, the amount of time the business has been open, and other indications of a legal, operating business. Byteworth personnel personally reviews and participates in the customer-onboarding and service-initiation process, and therefore is privy to their customer usage practices for voice calling and their related usage

practices.

Byteworth does not serve wholesale carrier customers. If it does, however, Byteworth acknowledges that its verification practices would be expanded to 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, along with a completed USF exemption certificate.

III. Byteworth's Acceptable Use Policy

Byteworth has an Acceptable Use Policy that, if violated, would lead Byteworth to investigate and, if appropriate, suspend and/or terminate a given customer's service in the event of a violation. Among other things, Byteworth prohibits unlawful usage, including unlawful telemarketing or prerecorded/artificial voice calls.

IV. STIR-SHAKEN Capabilities

Byteworth is a non-facilities-based reseller that lacks the necessary facilities and control over the network infrastructure necessary to implement STIR/SHAKEN, and therefore does not have a STIR/SHAKEN implementation obligation. *See Sixth Caller ID Authentication Report and Order* ¶ 36 & n. 137; *id.* ¶ 45 & n.170. Nevertheless, all of Byteworth'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/SHAKEN by that carrier partner.

V. Proactive Network Monitoring

Byteworth has various monitoring and reporting systems in place via its upstream carrier to analyze traffic on its network for potentially suspicious traffic patterns that are likely to be associated with illegal robocalls or other potentially unlawful or fraudulent usage. For example, Byteworth's upstream provider can monitor traffic and its CDRs based on various criteria, including data relating to call frequency per line, short-duration calls, answer-seizure ratios, call-failure ratios, and other anomalous call patterns.

If those systems and/or Byteworth detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, Byteworth will take prompt action to identify the party that is using its network to carry these calls and take appropriate action. Once suspected unlawful traffic is discovered, Byteworth will block any further traffic from being carried associated with the Media IP address of that suspicious traffic. In the event Byteworth discovers any suspicious traffic that is not demonstrably unlawful, Byteworth will complete its investigation, and their 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

Byteworth 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. Byteworth 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.