

Range Robocall Mitigation Plan^{**}

I. Introduction

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers, like Range Telecom (“Range”), 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*”), 47 C.F.R. § 64.6305(a)(2); *id.* at § 64.6305(b)(2)- (c)(2) (parallel rule for gateway and 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

^{**} As of the date of filing of this policy, Range is not carrying any calls or serving as a voice services provider. Range submits this policy to be in compliance with Commission regulations in the event it resumes carrying calls or serving as a voice services provider.

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)). Range 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, Range’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 (2011)) 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. Range is dedicated to developing and taking reasonable steps. This document outlines Range’s robocall mitigation plan.

II. Regulatory Compliance and Collaboration

1. Regulatory Adherence: We will comply with all relevant regulations, including the Telephone Consumer Protection Act (TCPA), Truth in Caller ID Act, and Federal Communications Commission (FCC) guidelines.
2. Collaboration with ITG: We will actively collaborate with ITG and other industry stakeholders to trace and mitigate robocalls. We will respond to all traceback requests within 24 hours.

III. Technology-Based Solutions

3. Range has fully implemented STIR/SHAKEN protocols to accurately authenticate caller IDs. Range will accurately sign, accept and transmit all STIR/SHAKEN data it receives in the call path, consistent with 47 C.F.R. § 64.6302-05
4. Robocall Detection: Range will deploy advanced machine learning algorithms to identify and block known spam callers and suspicious call patterns.
5. Caller Reputation Database: Range will maintain a comprehensive database to track the behavior of calling entities and enhance call authentication.

6. Media IP Reputation Database: Range will maintain a comprehensive database to track the behavior of calling IP's and enforce blocking when appropriate.

IV. Proactive Network Monitoring

Range will have 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, Range will monitor systems access and, as applicable, flag or automatically block, traffic based on various criteria, including

- matching NPA-NXXs of the calling and called parties' telephone numbers;
- blocking calls purporting to be from a telephone number on Somos' Do-Not-Originate list;
- blocking calls from any Media IP address associated with a known or reported illegal robocalling entity.
- In addition to its internal analytics and Somos DNO, Range will also subscribe to ZipDX's RRAPTOR product for monitoring insights.

7. If Range detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, Range will take prompt action to identify the party that is using its network to carry these calls and take appropriate action.

V. Ensuring We Know Our Customers

8. Range will make sure that it receives and thoroughly analyzes KYC forms from each customer. Analysis includes many steps – from verification of FRN number and Filer ID to a consistency of data across the KYC document, website, public databases, etc. Range will make sure each customer is a real business and they understand the requirements of the today's market when it comes to mitigation of malicious traffic.

VI. Three Strike Rule for Clients

9. Client Monitoring: Range will implement a robust client monitoring system to detect suspicious call traffic and behavior.

10. Three Strike Rule: Range will enforce a strict Three Strike Rule for clients who engage in suspicious or illegal call activities.

- ****Strike 1****: A warning is issued to the client for the first violation, educating them on compliance and the potential consequences.
- ****Strike 2****: Upon a second violation, the client faces temporary suspension of services, pending a review of their activities and adherence to regulations.
- **Strike 3**: A third violation results in the permanent termination of services for the client, and their activities are reported to relevant authorities.

VII. Traceback Response

11. Swift Traceback Handling: Range 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. Range 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.

VIII. Ongoing Monitoring and Improvement

12. Performance Metrics: Range will continuously monitor and analyze the effectiveness of our mitigation efforts, using key performance indicators (KPIs) to measure success.

13. Feedback Loop: Range will establish a feedback mechanism for consumers to report false positives/negatives, enabling continuous improvement.

IX. Transparency

14. Regular Reporting: Publish regular reports outlining our actions to mitigate robocalls, including traceback efforts and Three Strike Rule enforcement.

X. Collaboration

15. ****Multi-Stakeholder Collaboration****: Collaborate with industry peers, regulatory authorities, and law enforcement agencies to share information and best practices for combating robocalls.

XI. Resource Allocation

16. Resource Management: Allocate necessary resources, including personnel, technology, and budget, to support the successful execution of this plan.

XII. Review and Adaptation

17. Periodic Review: Regularly review the effectiveness of the plan, adapting to emerging threats, regulatory changes, industry developments, and client adherence to the Three Strike Rule.

Our Robocall Mitigation Plan, which includes a Three Strike Rule for clients, reflects our commitment to combating robocalls and ensuring compliance with regulations. By combining regulatory compliance, technological solutions, user education, reporting, a Three Strike Rule for clients, collaboration, transparency, and continuous improvement, we aim to significantly reduce the impact of unwanted automated calls and safeguard the integrity of voice communication.