

FS TELECOM, LLC
ROBOCALL MITIGATION PLAN

I. Background

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

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 (b) or (e) of section 227 of the Communications Act of 1934.”

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

Thus, FS Telecom’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 provide 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. FS Telecom only uses the internal analytics (using that term in its ordinary, undefined sense) identified herein.

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 of illegal robocalls, and the voice service provider complies with the practices described in its plan. *Sixth Caller ID Authentication Report and Order* ¶ 31. FS Telecom is dedicated to developing and taking reasonable steps. This document outlines FS Telecom’s robocall mitigation plan.

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

FS Telecom provides enterprise-grade voice and messaging services designed specifically for B2B sales engagement and compliant outbound communications. FS Telecom undertakes commercially reasonable measures to validate customer identity, intended use, and information regarding their compliance with applicable laws and industry standards before activating any telecom services.

All prospective customers complete a structured enrollment process, which may include a video or telephonic verification session with our onboarding team. As part of this process, FS Telecom verifies the prospective customer’s business by evaluating public and private information sources, such as:

- Confirmation of business name, trade names, and/or DBAs,
- Verification of company email domain, phone number, and website,
- Proof of incorporation (state, federal, or international business registration),
- Verification of a physical business address, and
- Identification of authorized contacts for telecom operations.

In addition, FS Telecom collects business-use details relevant to compliance, which can include:

- Nature of the customer's business, sales campaigns, and outreach strategies,
- Typical acquisition methods for lead lists or call targets,
- Whether communications are live-agent only or include other outreach types,
- Scrubbing practices related to the National Do Not Call (DNC) Registry, wireless numbers, and other consumer-protection frameworks.

III. FS Telecom's Acceptable Use Policy

As part of its customer-onboarding process, FS Telecom's customers contractually agree to various terms and conditions, including a commitment to comply with FS Telecom's Acceptable Use Policy (AUP). Among other things, FS Telecom customer cannot:

- Use FS Telecom services for any illegal, abusive, fraudulent, deceptive, or misleading activity, including those that exploit or endanger vulnerable populations.
- Engage in unsolicited advertising or unlawful marketing campaigns in violation of applicable laws, 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 Sales Rule (16 C.F.R. § 310 et seq.),
 - The Telephone Consumer Protection Act (TCPA, 47 U.S.C. § 227) and FCC regulations,
 - Federal and state Do Not Call (DNC) lists and calling-time restrictions.
 - Operate in violation of industry best practices and standards, such as the CTIA Messaging Principles and Best Practices.
 - Misrepresent caller identity, falsify headers, spoof numbers, or otherwise violate the Truth in Caller ID Act.

Violations of this AUP may result in immediate suspension or termination of service.

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

FS Telecom has fully implemented the STIR/SHAKEN authentication framework across its entire network, and all calls for which it serves as the originating provider are compliant with 47 C.F.R. Sec. 64.6301(a)(1)-(2).

FS Telecom Customers are authorized to use the numbers provisioned directly by FS Telecom, and if a customer seeks to use numbers obtained from another provider, FS Telecom requires documentary evidence (Letter of Authorization, invoice, or contract) proving rights to those numbers. These measures help ensure FS Telecom customers cannot engage in illegal spoofing or caller ID misrepresentation.

V. Proactive Network Monitoring and Analytics

FS Telecom employs continuous monitoring systems to detect abnormal or potentially unlawful traffic. Metrics include call duration patterns, Answer-Seizure Ratios (ASR), call failure codes, and anomalous number usage (ANI cardinality). Its systems are configured to detect activity consistent with illegal robocalling, spam campaigns, or spoofing attempts. If identified, FS Telecom acts quickly to:

- Investigate and isolate the customer traffic in question,
- Validate customer representations against actual call recordings or logs, and
- Suspend or terminate offending traffic as needed.

FS Telecom dedicates resources—including regulatory counsel specializing in TCPA and telecom law—to ensure its practices remain aligned with evolving federal and state requirements. FS Telecom does not deploy any third-party robocall analytics products.

VI. Commitment to Timely Traceback Responses and Cooperation

FS Telecom 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. FS Telecom 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.

**Addendum re Commission Action
re Deficient Robocall Mitigation Database Certification of TalkCycle LLC**

FS Telecom answered the following question on its RMD Certification with a “Yes”:

The filing entity has, at any time in the prior two years, been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

FS Telecom is therefore asked to provide the following information regarding that matter, which it provides below:

Provide a description of any such action or investigation, including all law enforcement or regulatory agencies involved, the date that any action or investigation was commenced, the current status of the action or investigation, a summary of the findings of wrongdoing made in connection with the action or investigation, and whether any final determinations have been issued.

Mr. Salame, a principal of FS Telecom, also has an ownership in TalkCycle LLC, which had an RMD entry (RMD0006079) that was removed by the FCC Enforcement Bureau’s August 25, 2025 Order in *In re Robocall Mitigation Database Filers*, EB-TCD-25-00038590, DA 25-737.

That action was commenced on December 10, 2024 via an email from the Enforcement Bureau on which Mr. Salame was bcc’ed, which email included a copy of the Order entered in *In re 2,411 Robocall Mitigation Database Filers*, EB-TCD-24-00036891, DA 24-1235. That Order stated that “Each Company’s RMD certification [including TalkCycle’s] is deficient because (a) a robocall mitigation plan was not provided or the plan lacks newly-required information; and (b) the certification lacks newly-required information.” The email from Mr. Rojo transmitting that Order stated that “Please find attached an Order released by the Enforcement Bureau of the Federal Communications Commission pertaining to deficiencies in your Robocall Mitigation Database certification.”

By email dated December 17, 2024, the Enforcement Bureau’s Ms. Kinsey bcc’ed Mr. Salame on an email that stated “Please find attached a Public Notice released by the Enforcement Bureau (Bureau) of the Federal Communications Commission announcing that a summary of the Bureau’s Order pertaining to deficiencies in your Robocall Mitigation Database certification has been published in the Federal Register,” and included a copy of the Bureau’s Public Notice DA 24-1267, which stated, among other things:

By this Public Notice, the Enforcement Bureau (Bureau) announces that on

December 17, 2024 a summary of the Bureau's order (Order) directing 2,411 voice service providers and gateway providers (each, a Company; collectively, the Companies) to show cause why they should not be removed from the Robocall Mitigation Database (RMD) was published in the Federal Register. Each Company named in Appendix A to the Order must file its response by December 31, 2024. Each Company must cure the deficiencies in its RMD certification and notify the Bureau that the deficiencies have been cured or file a response explaining why the Bureau should not remove the Company's certification from the RMD.

Regrettably, both of those emails went to Mr. Salame's spam folder, TalkCycle accordingly did not address the Bureau's Order or Public Notice, and thus the Bureau's August 25, 2025 Order constituted final Bureau action removing TalkCycle's RMD entry from the public-facing database because TalkCycle had "not cure[d] the deficiencies in their RMD certifications and notify the Bureau that the deficiencies have been cured; or [] file[d] a response with sufficient explanation for why the Bureau should not remove the Company's certification from the RMD." FS Telecom understands those to be the Bureau's final determinations regarding TalkCycle's RMD entry that had become deficient through lack of timely updates to comply with the FCC's later orders. TalkCycle's 2021 RMD entry was therefore removed on August 25, 2025, and it is understood that matter is final. Through counsel, TalkCycle conferred with Enforcement Bureau Staff after becoming aware of the August 25, 2025 Order, and amended its now-private RMD entry. FS Telecom understands that matter vis-à-vis TalkCycle to be final and concluded.