



ROBOCALL MITIGATION PLAN

1. Background

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers, like Dial Fusion, Inc. (“Dial Fusion”), to, among other things, file certifications and robocall mitigation plans in the FCC’s Robocall Mitigation Database (“RMD”). 47 CFR § 64.6305.

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 robocalls that use its service to originate calls.” 47 C.F.R. § 64.6305(a)(2).

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. Dial Fusion is dedicated to developing and taking reasonable steps. This document outlines Dial Fusion's robocall mitigation plan.

2. Due Diligence

Dial Fusion undertakes various commercially reasonable precautions to verify a given customer’s identity as part of entering into a formal written agreement. Dial Fusion collects and, as appropriate, verifies, as part of its processes certain customer information such as the customer business name, physical business location, contact person(s), and email address.

As of this filing, Dial Fusion has never received a traceback or carrier complaint about any robocall-related issue on any of its traffic.

i. See <https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf> (WCB Jan. 25, 2024 Public Notice).

3. Prohibited use of services and system.

As part of its customer-onboarding process, all of Dial Fusions' customers contractually agree to various terms and conditions, including a commitment to abide by certain restrictions. All consumers are prohibited from doing any of the following:

- Any unauthorized use of the System, or the resale, or attempt to resell the System, is expressly prohibited.
- Use the System in connection with chain letters, junk email, pyramid schemes, illegal or unethical testimonials, cross soliciting, money games, spamming, or any duplicative or unsolicited messages (commercial or otherwise);
- Harvest or otherwise collect information about others, including without limitation phone numbers and/or email addresses, without their consent.
- Create a false identity or forged email, or otherwise attempt to mislead others as to the identity of the user or the origin of the message.
- Transmit through the System unlawful, harassing, libelous, abusive, threatening, harmful, vulgar, obscene, or otherwise objectionable material of any kind or nature.
- Transmit any material that may infringe the intellectual property rights or other rights of third parties, including trademark, copyright or right of publicity.
- Libel, defame or slander any person, or infringe upon any person's privacy rights.
- Transmit any material that contains viruses, Trojan horses, worms, time bombs, cancel bots, or any other harmful or deleterious programs.
- Violate any U.S. law regarding the transmission of technical data or software exported from the United States through the System.
- Interfere with or disrupt networks connected to the System or violate the regulations, policies, or procedures of such networks.
- Attempt to gain unauthorized access to the System, other accounts, computer systems or networks connected to the System, through password mining or any other means.
- Interfere with another's use and enjoyment of the System or another entity's use and enjoyment of similar services.
- Transmit unsolicited commercial email or "spam," as defined in the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM" Act) (15 U.S.C. §7701) or, if applicable, Canada's Anti-Spam Law ("CASL"), illegally create or collect e-mail addresses, deceptively use e-mail relays or transmissions, or otherwise violate the CAN-SPAM Act or CASL; or
- Use the System to receive, send, or otherwise process Protected Health Information as defined by the Health Insurance Portability and Accountability Act of 1996 as amended, unless You have signed a Business Associate Agreement with Dial Fusion, or Your use of the System fits within the "conduit" or some other exception for requiring a Business Associate Agreement; or
- Use the System to record or monitor a phone call or other communication without securing consent from the participants to the phone call or other communication as required under applicable law (including, as applicable, California's Invasion of Privacy Act and similar laws in other jurisdictions); or

-
- Transmit SMS without the consent of the message recipient, who must agree to receive messages of the type you are going to send them, or otherwise fail to comply with any federal, state, or local laws; or
 - Engage in any other activity that might subject either You or Us to criminal liability, money judgments or other civil penalties.

4. STIR/SHAKEN Capabilities.

Dial Fusion is exempt from STIR/SHAKEN under 35 FCC Rcd. 3241, Para.40, and 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 also, Sixth Caller ID Authentication Report and Order* ¶ 36 & n. 137; *id.* ¶ 45 & n.170.

5. Proactive Network Monitoring.

Dial Fusion uses both automated and manual monitoring 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. If Dial Fusion detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, Dial Fusion will take prompt action to identify the party and take appropriate action.

6. Commitment to Timely Traceback Responses and Cooperation.

Dial Fusion commits to fully responding within 24 hours to all traceback requests from the Industry Traceback Group, the Traceback and Prevention Task Group, the FCC, and law enforcement. Dial Fusion shall cooperate with these groups to investigate and stop any illegal robocallers from using the Dial Fusion services to carry or process illegal calls.