

Nova Labs Robocall Mitigation Plan

Business Information

Nova Labs, Inc.
2261 Market Street, STE 10194
San Francisco, CA 94114

Contact Information

Sarah Aberg
General Counsel
(214) 814-2066
Saberg@nova-labs.com

Overview

Nova Labs, Inc. (“Nova Labs”) is a small voice service provider committed to preventing and mitigating illegal robocalls. Nova Labs is a mobile virtual network operator (“MVNO”) that relies on a major carrier’s network to provide voice service. Therefore, Nova Labs does not maintain ultimate control over the facilities/network infrastructure necessary to implement the STIR/SHAKEN framework and is not required to do so.¹

Despite not being required to implement STIR/SHAKEN, Nova Labs is fully committed to adhering to the FCC’s robocall mitigation directives, as applicable. As a threshold matter, Nova Labs notes that MVNO services are not well suited to the use of automatic dialing systems (which are prohibited by Nova Labs’ Acceptable Use Policy) and placing a high volume of calls. Accordingly, Nova Labs is not a significant risk of originating illegal robocalls.

Consistent with the Commission’s rules, this Robocall Mitigation Plan (“RMP”) outlines the "reasonable steps" Nova Labs undertakes to prevent the origination, carrying, or processing of illegal robocalls, including its "know your customer" and "know your upstream provider" procedures, as well as details about its call analytics system.²

Subscriber Due Diligence/“Know Your Customer”

Nova Labs implements procedures to accurately identify and authenticate subscribers. Information collected from subscribers includes full names, email addresses, billing details, and device identifiers. Nova Labs’ fraud protection systems also use this information to monitor potential fraud risks.

¹ See *Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources*, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3260, ¶ 40 (2020).

² See *Call Authentication Trust Anchor*, Sixth Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 17-97, FCC 23-18, at ¶¶ 29, 36-52 (Mar. 17, 2023); 47 C.F.R. § 64.6305.

Nova Labs' Terms of Service specifically prohibits unlawful or fraudulent uses of its services and specifically, the use of auto dialers on its network. Nova Labs' subscribers are required to adhere to an Acceptable Use Policy, accessible at: <https://hellohelium.com/acceptable-use>. As necessary, Nova Labs will suspend or terminate service to subscribers who violate these policies.

Know Your Upstream Providers

Nova Labs' upstream provider is T-Mobile USA, Inc., headquartered at 12920 S.E. 38th Street, Bellevue, WA 98006. While there are no formal contractual provisions between Nova Labs and its upstream provider regarding robocall mitigation, T-Mobile has confirmed to Nova Labs that it is compliant with STIR/SHAKEN and T-Mobile is listed as STIR/SHAKEN compliant in the FCC's robocall mitigation database.³ T-Mobile and Nova Labs work together to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Call Analytics for Monitoring Traffic and Governance Procedures

Nova Labs works with T-Mobile, its upstream provider, to monitor and analyze call patterns for signs of robocall activity. This system flags unusual call spikes and patterns, enabling the upstream provider to quickly identify and mitigate potential robocall threats.

T-Mobile has internal controls to prevent fraud, including robocalls. Nova Labs has set up a secure SFTP connection and is able to receive fraud alerts from T-Mobile, including automatically generated alerts and manual reports. When Nova Labs receives a fraud report, an immediate alert is distributed to key Nova Labs personnel responsible for addressing such alerts. All accounts that are found to be engaging in fraudulent activity or robocalls are cancelled immediately.

Additionally, Nova Labs has established internal monitoring tools and governance procedures to monitor traffic and detect potential robocall and robotext activity. Pattern of Practice Reviews are recorded in Nova Labs' Compliance Ticketing Notion Application Page in order to ensure that action is taken and issues are remediated in a timely manner.

Multiple Governance Forums are in place to identify and escalate unwanted subscriber activity, including robocalls and robotexts. The Governance Forums include Anti-Gaming Meetings which occur twice per month (at a minimum), and quarterly Robocall and Robotext meetings with senior members of the Subscriber and Network businesses and Compliance, Legal, Product, Customer Support, Operations and Technology staff. A Legal and Compliance meeting is conducted 1-3 times per week, as necessary, to address ad-hoc issues and patterns of practice reviews.

Investigation of Suspicious Activity

In collaboration with T-Mobile, Nova Labs promptly investigates suspicious or fraudulent network

³ *T-Mobile USA, Inc. Robocall Mitigation Database Registration*, available at https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robocall_mitigation_database&sys_id=a5d28f6d1bcd74109294113d9c4bcb98&view=sp.

activity. This includes, as appropriate, participating in traceback investigations, verifying subscriber number ownership, and taking necessary actions against identified threats. Where necessary, Nova Labs addresses the suspicious activity with appropriate remedial measures, which can include suspension or termination of service.

Information on T-Mobile processes for identifying and mitigating spam calls is described here:

<https://www.t-mobile.com/benefits/scam-shield-app> (consumer page).

<https://www.t-mobile.com/business/solutions/call-protection> (business page).

Traceback and Blocking

Nova Labs commits to respond within 24 hours to all lawful traceback requests and maintains a single point of contact for law enforcement and regulatory entities in order to efficiently respond to such requests. Nova Labs works with T-Mobile to address any Do Not Originate requests it receives from the Industry Traceback Group (“ITG”). Nova Labs will coordinate with the ITG, FCC, law enforcement, and other voice service providers to promptly address instances of suspected illegal robocalls or suspicious traffic. Nova Labs also maintains records of any traceback requests it receives, including the relevant parties involved in the requests.

Plan Updates

Recognizing the evolving nature of telecommunications fraud, Nova Labs will update this plan in line with industry best practices and regulatory requirements. Any material changes will be updated in the FCC Robocall Mitigation Database within ten (10) business days of such update.
