

Safety NetAccess, Inc.

Caller ID Authentication Plan

As of January 13, 2025

Introduction. Safety NetAccess, Inc. (“Safety NetAccess”), pursuant to Sections 64.6301 and 64.6305 of the Commission’s rules, 47 C.F.R. §§ [64.6301](#), [64.6305](#) and the Commission’s “Best Practices”¹ as amended² adopts this amended Caller ID Authentication (“Plan”). This Plan is current as of its submission date and may be subject to change as necessary to further comply with amended Commission regulations and requirements.

Exemption. Safety NetAccess falls under a plain language definition of a Small Voice Service Provider serving less than 100,000 voice service subscriber lines, pursuant to Section 64.6304(a)(2) of the Commission’s rules, [47 C.F.R. § 64.6304\(a\)\(2\)](#), albeit lacks control over network infrastructure necessary to implement STIR/SHAKEN.³ Safety NetAccess is currently incapable of obtaining a Service Provider Code (“SPC”) token due to Governance Authority policy and is exempt from the requirements of [Section 64.6301](#) until it is capable of obtaining a SPC token as set forth in Section 64.6304(b) of the Commission’s rules, 47 C.F.R. § 64.6304(b).

Commitment. Pursuant to Section 64.6305 of the Commission’s rules, 47 C.F.R. § [64.6305](#), Safety NetAccess commits to take all such *reasonable steps* to avoid originating illegal robocall traffic and shall include a commitment to respond fully and in a timely manner 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. As set forth below, Safety NetAccess has adapted the North America Numbering Council Call Authentication Trust Anchor Working Group’s *Best Practices for the Implementation of Call Authentication Frameworks*⁴ into its Plan.

¹ *Call Authentication Trust Anchor*, WT Docket No. 17-97 *Wireline Competition Bureau Invites Comment on Caller ID Authentication Best Practices*, WC Docket No. 20-324, *Wireline Competition Bureau Issues Caller ID Authentication Best Practices*, DA 20-1526 (December 22, 2020)

² *Advanced Methods to Target and Eliminate Unlawful Robocalls*, *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17- 97, *Sixth Report and Order*, *Fifth Report and Order*, *Order on Reconsideration*, *Order*, FCC 22-37 (May 20, 2022) and *Call Authentication Trust Anchor*, WC Docket No. 17-97, *Sixth Report and Order*, FCC 23-18 (March 17, 2023).

³ *Call Authentication Trust Anchor*, *Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 and 20-67, *Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd 3260 (Mar. 31, 2020) (First Caller ID Authentication Report and Order and Further Notice), para. 40.

⁴ *Public Notice*, WC Docket Nos. 17-97 and 20-324, [DA 20-1526](#), Appendix B (December 22, 2020)

Company Contact. The name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues is as follows:

Todd Shobert
Chief Technical Officer
Safety NetAccess, Inc.
1 University Avenue, Suite 103
Westwood, MA 02090
Telephone: 617.268.1134
Email: todd@safetynetaccess.com

Corporate Information. Safety NetAccess provides cloud PBX services for clients. PBX software is hosted in the cloud and managed by Company voice technicians. Safety NetAccess installation and support teams configure the software to provide standard telecom services for companies. Safety NetAccess uses Session Initiation Protocol trunks for voice services and customer broadband circuits to provide services to the end users. In no circumstances is the PBX software configured in a manner that would permit robocalling.

As Safety NetAccess broadens its provision of IP enabled services now including voice over Internet protocol telephony, Safety NetAccess incorporates additional robocall mitigation procedures set forth herein, to ensure its ongoing compliance in precluding any potential for robocalling through its broadened service offerings.

Safety NetAccess operates exclusively as a non-facilities-based Small Voice Service Provider as defined, with a STIR/SHAKEN implementation obligation serving end-users as set forth herein. Safety NetAccess does not operate under any assumed names. Safety NetAccess is not a foreign voice service provider, is not an intermediate or gateway provider, and does not serve subscribers who are physically located outside of the U.S. Safety NetAccess does not maintain an operating company number and does not have direct access to telephone numbers from the North American Numbering Plan Administrator (NANPA) and/or the National Pooling Administrator.

Safety NetAccess certifies that it has not been prohibited from filing in the Robocall Mitigation Database. Safety NetAccess certifies further that it has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing. And Safety NetAccess certifies that at no time during the prior two years, has Safety NetAccess 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 transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

Reasonable Steps to Prevent Robocalling.

Subscriber Vetting

Safety NetAccess fully vets all subscribers before providing service to the subscriber. Safety NetAccess obtains specific subscriber information including service locations and principals if commercial subscribers, and verifies location for all subscribers. Further, Safety NetAccess compares information provided by the subscriber against underlying carrier records to verify accuracy and authentication and validate subscriber information. Subscribers are served under a service agreement.

Safety NetAccess monitors its subscribers' traffic for call, originating number and terminating number irregularities in conjunction with its underlying carriers, and should irregularities be determined, will immediately contact the subscriber as part of its investigatory process. Safety NetAccess does not grant, nor can it grant, right-to-use telephone number resources.

Telephone Number Validation

For new subscribers, Safety NetAccess will assign telephone numbers to the account through its numbering partner, unless the account has ported from another subscriber. Safety NetAccess will ensure that only those subscriber telephone numbers held by its subscribers may originate traffic. For toll-free numbers, Safety NetAccess will verify the underlying ten-digit number and ensure that only calls from the assigned numbers may originate calls.

Network Traffic Monitoring, Analysis and Investigation.

Consistent with its commitment above, Safety NetAccess will respond fully to all traceback requests from the Commission, law enforcement, and the industry traceback consortium as soon as possible and at no time exceeding 24 hours from the time of the request and will cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Safety NetAccess coordinates with its underlying carriers, Bandwidth and Voyant, to investigate suspicious subscribers' traffic, identify traffic anomalies including, but not limited to, unusually high call volumes to different telephone numbers and disparate geographic areas, over the course of one or more hours, for which Safety NetAccess will investigate, and to block subscriber service if robocalling is suspected. Confirmation of illegal activity and more than one violation will result in immediate service termination.

Refusing Traffic from Unlisted Providers.

In conjunction with its underlying carriers, Safety NetAccess refuses to accept traffic from unlisted and de-listed providers from the Commission's Robocall Mitigation Database.

Ongoing Robocall Mitigation.

Safety NetAccess, in conjunction with its underlying carriers, will implement a call authentication protocol for voice calls delivered over the non-IP portions of its network that do not use SIP technology when such a protocol is fully developed and finalized by industry standards and the necessary equipment and software is available on the commercial market.

Safety NetAccess anticipates that its Plan will evolve as it makes Plan enhancements, as underlying carriers enhance their own plans, and as the Trust Anchor and industry generally gain experience in caller ID authentication protocols.

Safety NetAccess avers to update its plan within ten business days from the date of any Plan changes.

Safety NetAccess, Inc.

/s/ Todd Shobert

Todd Shobert
Chief Technical Officer
Safety NetAccess, Inc.
1 University Avenue, Suite 103
Westwood, MA 02090
Telephone: 617.268.1134