

Smart Choice Communications, LLC

Caller ID Authentication Plan

Updated February 18, 2026

I. Introduction

Smart Choice Communications, LLC (“SCC”), Federal Registration Number 0008879306, 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 adopts this Caller ID Authentication (“Plan”) to prevent unlawful robocalls from originating, terminating, or being carried or processed on SCC’s voice networks

SCC has incorporated amendments to its Plan reflecting implementation of Commission rules promulgated under the Commission’s Sixth and Seventh Report and Order in its Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor proceedings.²

With this update, SCC incorporates amendments to its Plan to further document compliance with Commission Caller ID Authentication rules, most recently including rules promulgated under the *Report and Order* in its Improving the Effectiveness of the Robocall Mitigation Database and Amendment of Part 1 of the Commission’s Rules, Concerning Practice and Procedure, Amendment of CORES Registration System proceedings.³

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.

II. Company Information

The name, title, department, business address, telephone number, and email address of the individual within the company responsible for addressing robocall mitigation-related issues is:

Basil Stepanov
Chief Technology Officer
Smart Choice Communications
145 east 45th street
New York, NY 10036
Telephone: 800.217.3096
Email: regulatory@smartchoiceus.com

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, *Six Report in Order*, FCC 23-18 (rel. Mar. 19, 2023) (“Sixth Report and Order”), and *Seventh Report and Order* (rel. May 19, 2023) (“Seventh Report and Order”).

³ *Report and Order*, WC Docket No. 24-213, MD Docket No. 10-234, [FCC 24-135](#) (January 8, 2025),

II. Company Information, Continued

SCC provides local, intrastate, interstate, and international telecommunications and communications service, and enhanced services to commercial and residential subscribers in several states. SCC falls under a plain language definition of a Small Voice Service Provider serving less than 100,000 voice service subscriber lines, as defined in Section 64.6304(a)(2) of the Commission's rules, 47 C.F.R. § 64.6304(a)(2).

SCC is a privately-owned corporation. SCC's individual owner and principal is Jarrett Wolfe, President. SCC has no affiliates, has no subsidiaries, and is not owned by any other entity. The Company's principal exerts full control over SCC's operations.

SCC does not operate under any assumed names. SCC is not an Intermediate nor Gateway provider, and does not serve subscribers who are physically located outside of the U.S. and do not maintain U.S. offices.

SCC maintains operating company numbers 416B, 041G, 042G, 175G, 176G, 216B, and 217B. SCC does not have direct access to telephone numbers from the North American Numbering Plan Administrator (NANPA) and/or the National Pooling Administrator.

III. Certification

SCC certifies that it maintains a service provider code token and that its originating calls are authenticated through [TransNexus](#). SCC has also deployed analytics applications that automatically analyze subscriber traffic for calling pattern anomalies that could be the result of robocalling subject to company investigation.

SCC certifies further that it has not been prohibited from filing in the Robocall Mitigation Database. SCC 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 SCC certifies that at no time during the prior two years, has SCC 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.

IV. Robocall Mitigation Plan

This Robocall Mitigation Plan addresses the steps SCC has implemented to eliminate unlawful calls originating on its network, in compliance with applicable Commission rules including:

- Know Your Customer
- Subscriber Vetting
- Contractual Provisions to Mitigate Robocalls
- Caller ID Authentication
- Telephone Number Validation
- Network Traffic Monitoring, Analysis, and Investigation
- Cooperation with the Commission, Industry Traceback Consortium, and Law Enforcement Agencies

IV. Robocall Mitigation Plan, Continued

Know Your Customer

SCC has adopted a multi-faceted approach for knowing its subscribers, beginning with a prospective subscriber's initial interaction with SCC's sales team. SCC's sales personnel undergo rigorous training to identify and screen potential customers effectively. When onboarding prospective subscribers, SCC conducts thorough credit checks to ensure not only the financial viability of the Subscriber but as an extra layer of security against fraudulent or questionable entities.

SCC project managers engage in weekly calls with new subscribers prior to the installation process, fostering open communication and addressing any concerns proactively. This ongoing dialogue allows SCC to stay attuned to our clients' evolving needs while simultaneously providing an opportunity to identify and address any potential issues that may arise.

By implementing such a robust program, SCC precludes serving companies that could engage in unlawful robocallers, telemarketers, cold callers, auto dialers, or any other malicious entities.

Subscriber Vetting

SCC exclusively serves commercial subscribers. SCC has a long-standing relationship with its commercial wholesale and retail subscribers. For all subscribers, including new subscribers, SCC assigns an in-house account manager who is responsible for managing SCC's relationship with each subscriber and who fully vets the subscriber before SCC begins to provide service to the subscriber, as set forth above.

SCC obtains specific subscriber information including service locations, principals, and credit information. Subscribers are served under Master Service Order and Service Level Agreements. The account manager will maintain periodic contact with the account contact.

SCC will obtain wholesale customers' FCC Form 499 filer ID in anticipation of initiating a relationship. The Company establishes usage thresholds as the basis for planning and monitoring wholesale subscriber traffic.

SCC will perform subscriber vetting for international subscribers as set forth above. SCC's international subscribers all maintain U.S. locations.

Contractual Provisions to Prohibit Robocalls

SCC includes contractual language in its wholesale agreements requiring subscribers to comply with the Commission's call authentication rules and Robocall Mitigation Database certifications. Further, SCC will verify that its wholesale service subscribers appear in the Commission's Robocall Mitigation Database and will confirm each wholesale subscriber's robocall mitigation compliance.

Retail subscribers are subject to SCC's terms and conditions, which expressly prohibits unlawful actions, including robocalling, and its Acceptable Use Policy, <https://smartchoiceus.com/acceptable-use-policy/>.

SCC retains the right to immediately suspend or terminate service without notice for violations of its Acceptable Use Policy.

IV. Robocall Mitigation Plan, Continued

Caller ID Authentication

Pursuant to Section 64.6301, Caller ID Authentication, 47 C.F.R. §§ 64.6301, SCC authenticates and verifies caller information for calls through its engagement of Transnexus in conjunction with SCC's Service Provider Code (SPC) token assigned by iconectiv.

Transnexus, authenticates calls generated over SCC's network using SCC's assigned SPC token. All domestic and international calls originating from SCC's network are authenticated, accordingly.

By incorporating this advanced certificate signing mechanism into its outbound call process, SCC not only mitigates the risk of fraudulent activities such as caller ID spoofing but also establishes a reliable and secure framework for all our customers. In so doing, SCC fully implements the STIR/SHAKEN authentication across its entire network and calls it originates are compliant with 47 C.F.R. §§ 64.6301.

Telephone Number Validation

For new subscribers, SCC assigns telephone numbers to the account through its numbering partner, unless the account has ported from another subscriber. SCC will ensure that only those subscriber endpoints and assigned numbers may originate traffic.

SCC performs number validation directly for traffic routed through its network and has established monitoring relationships with its underlying carriers to identify and investigate traffic anomalies.

Network Traffic Monitoring, Analysis, and Investigation

SCC has procedures to monitor traffic over its own network and algorithms that help identify traffic anomalies. SCC's network engineer is experienced in conducting traffic studies, analyzing traffic patterns and conducting root cause investigations. Further, SCC's network team is trained on robocall mitigation and coordinates with its underlying carriers to develop procedures for identification and investigation of changed patterns and potential instances of robocalling consistent with the underlying carriers' own caller ID authentication procedures.

Once SCC begins providing service to new subscribers, SCC engages in rigorous subscriber traffic analysis, to monitor the potential for anomalous traffic patterns. SCC monitors its subscribers' traffic for originating number and terminating number irregularities, call volume by time of day, and unusual call volume by destination. Should irregularities be determined, SCC will immediately contact the subscriber as part of its investigatory process to confirm the legitimacy of the calls.

Pursuant to the Commission's *Eighth Report and Order* in its Advanced Methods to Target and Eliminate Unlawful Robocalls proceeding,⁴ SCC expanded its reasonable do-not-originate list. SCC's do-not-originate list further excludes numbers that are deemed unreasonable for purposes of call origination in accordance with the criteria established pursuant to 47 C.F.R. § 64.1200.

⁴ *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Eighth Report and Order, FCC 25-15 (February 28, 2025) revising Section 64.1200(o) of the Commission's rules, [47 C.F.R. § 64.1200\(o\)](#).

IV. Robocall Mitigation Plan, Continued

Network Traffic Monitoring, Analysis, and Investigation, Continued

Specifically, SCC's enhanced do-not-originate list includes:

- **Multiple Fraud Triggers:** Automatically flags suspicious activity based on:
 - High call volume per minute
 - Mismatched caller IDs
 - Customer complaints
 - Customer blacklist requests
- **Automated Blocking:** Proprietary algorithms identify potential fraud and prevent suspicious numbers from calling in or being called out.
- **Customer Control:** End-users can add numbers to their personal blacklist for both inbound and outbound calls, ensuring a tailored layer of protection.
- **Proactive Defense:** Real-time monitoring and immediate call blocking to mitigate risks and protect both service providers and customers from fraudulent activity.

Cooperation with the Commission, Industry Traceback Consortium, and Law Enforcement Agencies

SCC avers to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium within twenty-four (24) hours,⁵ and to cooperate with such entities in investigating and stopping any illegal robocallers that use SCC's service to originate calls. SCC will coordinate with its wholesale subscribers for any traceback requests to ensure compliance.

If following internal investigation and investigation in conjunction with the industry traceback consortium, Commission, and/or law enforcement agencies, SCC confirms that any subscriber has engaged in – or allowed the engagement of – robocalling, SCC will immediately terminate its provision of service as a violation of its Acceptable Use Policy, <https://smartchoiceus.com/acceptable-use-policy/> and inform the Commission and Trust Anchor of the identity of the former subscriber and telephone numbers that were involved.

V. Commitment

Pursuant to Section 64.6305 of the Commission's rules, 47 C.F.R. § [64.6305](#), SCC 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, the industry traceback consortium, and underlying carriers, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

SCC will not accept traffic from any provider that has been removed from the Robocall Mitigation Database following Commission enforcement action, nor from providers who have not submitted robocall mitigation plans.

⁵ Pursuant to 47 C.F.R. § 64.1200(n)(1) as clarified by the Commission.

IV. Commitment, Continued

SCC 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.

SCC will ensure that it will update company information contained in the Commission Registration System (CORES) within ten business days from the date when information changes to reflect up-to-date Company information Further, pursuant to Section 64.6305(h) of the Commission's rules, 47 C.F.R. § 64.6305(h) SCC affirmatively certifies and will recertify annually, that any information submitted to the Robocall Mitigation Database is true and correct on or before March 1.

February 18, 2026

Smart Choice Communications, LLC

/s/ Basil Stepanov

Basil Stepanov
Chief Technology Officer
Smart Choice Communications
145 east 45th street
New York, NY 10036
Telephone: 800.217.3096