Robocall Mitigation Program Description

Shield Networks, Inc. | FRN: 0039080627 | WC Docket No. 17-97
Submitted pursuant to 47 CFR § 64.6305(d) | Effective: October 29, 2026

1. Company Identification

- **Legal name:** Shield Networks, Inc.
- **Primary address:** 13760 Marchant Ave, Sylmar, CA 91342
- **Other business names in use:** None
- **Previous business names:** None
- **Foreign voice service provider:** No. Shield Networks, Inc. is a U.S. company serving U.S. customers.
- **Robocall mitigation contact:** Alex Areg Mkrtchyan, Chief Executive Officer, Executive Office; 13760 Marchant Ave, Sylmar, CA 91342; 818-233-0102; info@shieldnetworksolutions.com

2. Principals, Affiliates, Subsidiaries, and Parent Companies

- **Principals:** Alex Areg Mkrtchyan, Chief Executive Officer (sole principal).
- **Parent company:** None
- **Subsidiaries:** None
- **Affiliates:** None
- No principal, affiliate, subsidiary, or parent of the company has been prohibited from filing in, or had a certification removed from, the Robocall Mitigation Database.

3. Role in the Call Chain and STIR/SHAKEN Status

Shield Networks, Inc. is a voice service provider serving business end-users and does not have a STIR/SHAKEN implementation obligation. Shield Networks resells hosted PBX/UCaaS service to small and mid-sized business customers. Shield Networks does not own or operate any switching equipment, session border controller, or call-signing infrastructure.

- **PBX platform:** Customer PBX tenants are hosted and operated by a third-party hosted PBX platform provider on that provider's infrastructure.
- **Upstream carrier:** All outbound calls are delivered via SIP trunks to a single upstream facilities-based carrier that controls the network edge where STIR/SHAKEN authentication occurs and signs Shield Networks' outbound calls.
- **Exemption:** Shield Networks lacks control of the network infrastructure necessary to implement STIR/SHAKEN. See Call Authentication Trust Anchor, Report and Order, 35 FCC Rcd 3241, 3260, para. 40 (2020); Second Report and Order, 36 FCC Rcd 1859, 1868, para. 19 (2020); Sixth Report and Order, FCC 23-18, para. 17 (2023).
- **Other roles:** Shield Networks does not act as a gateway or intermediate provider, does not offer wholesale origination, and does not accept traffic from other voice service providers.

4. Services Offered and Prohibited Uses

Shield Networks provides business telephone service (extensions, inbound DIDs, outbound calling, voicemail, auto-attendants) to established businesses, generally under ongoing managed IT service relationships. Shield Networks does **not** offer or knowingly permit:

- Outbound telemarketing, call-center dialing, predictive or auto-dialer platforms, or bulk/broadcast voice campaigns;
- Prerecorded or artificial-voice (including AI-generated voice) calls without the prior express consent required by law;
- Caller ID values not assigned to, or verifiably authorized for use by, the customer;
- Resale of Shield Networks service to other providers or third parties.

5. Know-Your-Customer: New and Renewing Customers

Shield Networks takes the following affirmative, effective measures to prevent new and renewing customers from originating illegal calls:

Before service activation (new customers):

- Collect and verify the customer's legal business name, EIN, and physical business address;
- Confirm active registration with the applicable Secretary of State;
- Verify the identity of the authorized signatory with government-issued photo ID;
- Collect a description of intended calling use and expected call volume; any indication of high-volume outbound, telemarketing, or dialer use results in denial of service;
- Require payment through a method in the business's name;
- Require a signed service agreement incorporating Shield Networks' Acceptable Use Policy (Section 8).

Renewing and existing customers: KYC information is re-verified at each contract renewal and at least annually, and immediately upon a change of ownership, a material change in seat count or calling volume, a request for additional telephone numbers, or any anomaly flagged under Section 7. Customers who cannot be re-verified are suspended.

Red flags that trigger denial or suspension: unverifiable business identity, mismatched or virtual-only addresses, refusal to describe calling use, requests for large blocks of numbers or numbers in many area codes, and requests to present caller ID not assigned to the customer.

6. Telephone Number and Caller ID Controls

- Telephone numbers are assigned only from Shield Networks' number inventory with its upstream carrier or ported in with a verified Letter of Authorization from the number's current subscriber;
- Number quantities are limited to the customer's verified business need;
- Outbound caller ID is restricted at the PBX tenant level to numbers assigned to that customer; customers cannot set arbitrary caller ID values;
- Shield Networks does not permit calls presenting invalid, unallocated, unassigned, or Do-Not-Originate numbers as caller ID.

7. Traffic Controls, Monitoring, and Call Analytics

- **Capacity limits:** Each tenant's concurrent outbound calls are capped in proportion to its seat count, preventing high-volume dialing;
- **International calling:** Disabled by default; enabled only on documented business need, with destination restrictions;
- **Monitoring:** Shield Networks reviews call detail records at least weekly, and immediately upon any alert, for indicators of illegal robocalling: high call volume relative to seat count, high proportions of short-duration calls, low answer rates, sequential or randomized dialing patterns, after-hours spikes, and caller ID anomalies;
- **Third-party analytics vendor:** Shield Networks does not currently contract with a third-party call analytics vendor. It relies on the PBX controls and CDR review described above, together with any analytics applied by its upstream carrier.

8. Contractual Provisions with End-Users

Shield Networks' customer service agreement and Acceptable Use Policy:

- Prohibit illegal robocalls, caller ID spoofing, and any use violating the TCPA, the Telemarketing Sales Rule, the TRACED Act, or state law;
- Prohibit the uses listed in Section 4;
- Require the customer to cooperate fully and promptly with traceback requests and investigations;
- Authorize Shield Networks to suspend service immediately, without prior notice, upon suspected illegal calling, and to terminate service for violations.

9. Know-Your-Upstream-Provider

- Shield Networks' only upstream voice provider is a single facilities-based carrier, which Shield Networks has verified is listed in the Robocall Mitigation Database;
- Shield Networks does not accept voice traffic from any other provider;
- Before adding any new upstream or carrier partner, Shield Networks will verify that the provider is listed in the RMD, and Shield Networks re-verifies the RMD status of all carrier partners at least annually;
- Shield Networks will stop routing traffic to any partner whose RMD certification is removed.

10. Traceback Response and Cooperation

Shield Networks commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium (Industry Traceback Group), and to cooperate with these entities in investigating and stopping any illegal robocallers that use its service to originate calls. On receipt of a traceback request, Shield Networks will:

- Identify the originating customer using PBX and carrier call detail records;
- Respond through the requesting entity's designated channel with the required information;
- Suspend the implicated traffic or account pending investigation;
- Preserve all associated records.

The robocall mitigation contact in Section 1 monitors traceback requests, including on weekends and holidays.

11. Response to Suspected Illegal Traffic

When Shield Networks detects or is notified of suspected illegal calling (by its own monitoring, its upstream carrier, the Commission, law enforcement, or the Industry Traceback Group), it immediately suspends the implicated outbound calling, investigates, and terminates the customer where a violation is confirmed. Terminated customers are not re-onboarded.

12. Enforcement History

Shield Networks is not, and has not been, the subject of any Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

13. Records, Training, and Plan Maintenance

- **Records:** Shield Networks retains KYC records and call detail records for at least 24 months;
- **Training:** Personnel involved in onboarding and support are trained on this program;
- **Review:** Shield Networks reviews this program at least annually, before its March 1 RMD recertification;
- **Updates:** Shield Networks updates its RMD filing within 10 business days of any change to the information it contains.