

Certificate of Robocall Mitigation Policy

Polarstar LLC (DBA Touchpoints)

Filer Legal Name: **Polarstar LLC**

DBA: **Touchpoints**

Primary Compliance Contact: **Brian Nixon, Owner**

Email: brian@touchpointspro.com

Phone: **8013606362**

Business Address:

1967 Heather Rd

Orem, UT 84097

Date: **December 18th, 2025**

1. Overview

This Certificate is submitted on behalf of Polarstar LLC (DBA Touchpoints) to certify that, to the extent required to file in the FCC Robocall Mitigation Database (RMD), the calls associated with Touchpoints' service are subject to a Robocall Mitigation Program. This program is designed to prevent the origination, carrying, or processing of illegal robocall traffic based on Touchpoints' role in the call chain, and to ensure timely traceback cooperation consistent with the FCC's rules and filing requirements.

2. Service Description and Role in the Call Chain

Touchpoints is primarily a programmatic messaging platform that enables customers to send personalized application-to-person SMS/MMS.

Voice functionality within Touchpoints is limited to inbound call handling and routing instructions:

- Touchpoints receives notifications of inbound calls from an underlying voice service provider.
- Touchpoints then programmatically instructs the provider whether/where an inbound call should be routed (e.g., forwarded to a configured destination) or terminated.
- Touchpoints does not generate outbound voice calls and does not originate robocall campaigns.

3. STIR/SHAKEN Status (No Extension Claim Included Here)

Touchpoints does not sign calls with STIR/SHAKEN. Touchpoints' robocall risk controls are addressed through the Robocall Mitigation Program described below. If Touchpoints asserts that it does not have a STIR/SHAKEN implementation obligation (e.g., due to lack of control over the network infrastructure necessary to implement STIR/SHAKEN), Touchpoints will explicitly cite the applicable basis in its RMD submission and explain in detail why that basis applies.

4. Know Your Customer (KYC) Program

Touchpoints maintains and applies a KYC program that is used for (a) new customers prior to enabling programmatic messaging and/or voice routing features, and (b) existing customers through periodic and event-driven re-verification.

4.1 KYC – Data Collected at Sign-Up (New Customers)

During customer sign-up and onboarding, Touchpoints collects:

- Customer name (individual or business), physical address, and corporate status (where applicable).
- EIN for business customers where relevant (Touchpoints does not collect SSNs).
- Administrative contact information for authorized account users.
- A description of intended use (messaging purpose, industry, and expected volume).

4.2 KYC – Identity / Brand Verification via The Campaign Registry (TCR) (Messaging)

Where A2P 10DLC registration is required for U.S. messaging use cases, Touchpoints uses The Campaign Registry (TCR) brand/campaign registration and vetting process as a component of onboarding verification for messaging senders.

For individual/sole-proprietor registrations where applicable through TCR workflows, the customer must complete an OTP verification process using an SMS-enabled device (as required by the applicable registration workflow).

Note: TCR vetting is used as a messaging identity verification input and does not replace Touchpoints' independent monitoring and enforcement controls described in Section 5.

4.3 Applying KYC to Existing Customers

Touchpoints applies KYC to existing customers through:

- Periodic account verification reviews (risk-based; at least annually where practicable) to confirm customer identity/contact fields remain accurate and, where applicable, that required messaging registrations (e.g., A2P 10DLC) remain current.
- Event-driven reviews triggered by risk indicators including unusual volume bursts, customer complaints, suspected policy violations, or traceback/industry notices.

If an existing customer fails to provide required updated information or verification within a reasonable period, Touchpoints may restrict or suspend capabilities until verification is completed.

5. Specific Reasonable Steps to Mitigate Illegal Traffic (Monitoring + Enforcement)

Touchpoints employs affirmative controls designed to detect and mitigate illegal or abusive traffic consistent with its role:

5.1 Monitoring / Analytics

Touchpoints monitors outbound messaging activity in near real-time to identify suspicious or abusive behavior patterns, including unusual bursts/spikes in sending activity.

Third-Party Analytics Vendor Disclosure:

- Touchpoints does not currently use a third-party call analytics vendor for robocall detection.
- For messaging sender identity vetting/registration (A2P 10DLC), Touchpoints uses The Campaign Registry (TCR) as described in Section 4.2.

5.2 Mitigation and Enforcement Actions

When suspicious activity is detected, Touchpoints takes reasonable and appropriate enforcement actions, which may include:

- Automated or manual throttling / rate limiting of messaging activity.
- Temporary suspension of messaging features pending investigation.
- Disabling specific sending configurations associated with suspected abuse.
- Account termination for confirmed violations of law or policy.
- Where applicable, coordination with upstream providers and/or the ITG traceback consortium or law enforcement.

Operational Support:

Touchpoints provides telephone support coverage during business hours (9:00 AM–5:00 PM, Monday–Friday) to investigate suspected abuse, respond to escalations, and coordinate mitigation actions.

6. Traceback and Enforcement Cooperation (24-Hour Commitment)

Touchpoints commits to respond fully to traceback requests within 24 hours and to cooperate with the FCC, law enforcement, and the industry traceback consortium in investigating and stopping illegal robocallers that may attempt to use services associated with Touchpoints.

7. Recordkeeping

Touchpoints maintains records relevant to KYC, monitoring alerts, investigations, enforcement actions, and traceback responses for a reasonable period to support compliance and timely investigations.

Signed,
Brian Nixon
Owner
Polarstar LLC (DBA Touchpoints)