

Dot Internet Solutions Inc. (Canada) — Robocall Mitigation Plan (Redacted)

Version 1.0 (Redacted) | Date: February 13, 2026

This copy is intentionally redacted for public distribution. Personally identifiable information (PII) such as names, email addresses, and direct phone numbers has been removed.

1) Company Information & Filing Context

This Robocall Mitigation Plan (RMP) describes the policies, technical controls, and operational procedures used by Dot Internet Solutions Inc. (Canada) to prevent the origination of illegal robocalls. The company is a Canadian-based voice service provider whose outbound calls may terminate to U.S. NANP numbers via our upstream partner, SkySwitch (U.S.-based upstream).

2) STIR/SHAKEN Obligation Status

We certify that we are filing in the FCC Robocall Mitigation Database as a Voice Service Provider without a STIR/SHAKEN obligation. Our upstream provider performs all required caller ID authentication for calls entering the U.S. PSTN.

3) Basis for Exemption (Foreign Provider)

As a foreign provider under 47 CFR § 64.6305, we do not operate U.S. facilities nor directly interconnect with the U.S. PSTN. Our upstream partner performs STIR/SHAKEN on our behalf.

4) Upstream Caller ID Authentication

SkySwitch (U.S.-based upstream) performs STIR/SHAKEN authentication for calls entering the U.S. PSTN. We maintain controls to ensure correct identity, routing, and traceback compatibility.

5) Robocall Mitigation Program — Controls & Procedures

1. KYC validation for all clients.
2. Contracts that prohibit illegal robocalls and spoofing.
3. Caller ID validation and blocking of invalid ANI.
4. Traffic analytics to detect abnormal or high-risk patterns.
5. Rate limiting, gating, and automated suspension for suspicious traffic.
6. Abuse complaint handling with prompt investigation.
7. Full cooperation with traceback requests within 24 hours.
8. Record retention for at least 24 months.
9. Security controls including MFA and restricted access.

6) U.S. & Canadian Regulatory Alignment

We comply with FCC robocall mitigation rules and applicable CRTC requirements, applying the stricter framework when possible.

7) Designated Compliance Contacts (Redacted)

Role	Name	Email	Phone	Time Zone
Primary Compliance Contact	[REDACTED]	[REDACTED]	[REDACTED]	EST
24x7 Traceback/Escalation	[REDACTED]	[REDACTED]	[REDACTED]	EST

8) Incident Response Timeline

Trigger/Event	Target Response
Traceback request	Acknowledge in 4 hours; full reply in 24 hours
Abuse complaint	Triage within 4 hours; mitigation within 24 hours
High-risk alert	Automated gating; engineering review within 2 hours
Repeat violation	Immediate suspension and review

Appendix — References

- 47 CFR § 64.6305 — FCC Robocall Mitigation Requirements
- FCC Robocall Mitigation Database Portal
- CRTC STIR/SHAKEN Requirements and Telecom Rules