

Robocall Monitoring and Mitigation Policy

6321275 Canada Ltd. (DBA: Internet Infinity)

Operating Company Number (OCN): 463L

1. Purpose

This policy outlines Internet Infinity's practices for identifying, analyzing, and mitigating unlawful or suspicious robocall activity in compliance with regulatory and industry expectations.

This policy is designed to satisfy the robocall mitigation requirements outlined in 47 CFR § 64.6305(a), including a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium.

2. Scope

This policy applies to all SIP and voice traffic originating from, transiting through, or terminating on Internet Infinity's infrastructure, including traffic from direct clients and resellers.

3. Monitoring Practices

3.1. Traffic Pattern Analysis

We monitor SIP traffic using automated systems and manual sampling to detect:

- High-volume call bursts
- Abnormally short call durations (e.g., < 10 seconds)
- Invalid or spoofed caller ID formats
- Repeated calls to large blocks of numbers (sequential or random)

3.2. Signature and List Matching

Our platform compares signaling data and metadata against:

- Industry-provided robocall signature databases
- Known scam number lists (e.g., FTC, CRTC, CNAM anomalies)
- Internal blocklists built from prior enforcement activity

4. Client and Reseller Oversight

4.1. Vetting and Onboarding

All new clients and resellers undergo verification of business legitimacy, number ownership, and intended use of services.

4.2. Call Behavior Review

Clients are subject to ongoing behavioral profiling. Accounts exhibiting patterns indicative of robocalling or spamming are flagged for investigation.

4.3. Corrective Actions

Upon identification of suspicious activity:

- The account is reviewed and may be rate-limited or suspended
- The client is contacted and required to justify or cease the activity
- Persistent violators are terminated and upstreams may be notified

5. Caller ID Validation

Clients may only present numbers:

- Assigned by Internet Infinity (eligible for A attestation)
- Validated through our external number validation process (eligible for B attestation)
- Other numbers will receive C attestation or be blocked at our discretion

6. Traceback Cooperation

We fully cooperate with traceback efforts and use the data obtained to inform our risk models and blocklists.

7. Logging and Retention

Traffic data, CDRs, and mitigation logs are retained for a minimum of **12 months** for audit and traceback purposes.

8. Review and Enforcement

This policy is reviewed **annually** and updated as industry standards evolve. Internal staff are trained to enforce mitigation processes consistently and responsibly.