

Robocall Mitigation Plan

Entity Name: Johns Creek Computers

FRN: 0038210316

Date: May 15, 2026

1. Purpose and Scope

This Robocall Mitigation Plan (RMP) outlines the "reasonable steps" taken by **[Your Company Name]** to prevent the origination, transit, or termination of illegal robocall traffic on its network. This plan is designed to comply with 47 C.F.R. § 64.6305 and the Federal Communications Commission's (FCC) Robocall Mitigation Database (RMD) requirements.

2. Know-Your-Customer (KYC) Protocols

To prevent illegal robocallers from accessing the network, **[Your Company Name]** implements the following vetting procedures:

- **Identity Verification:** We collect and verify physical business addresses, primary contact information, and Taxpayer Identification Numbers (TIN/EIN) for all new commercial customers.
- **Business Nature Review:** We assess the nature of the customer's business to ensure their expected traffic patterns align with legitimate business operations.
- **Contractual Prohibitions:** Service agreements explicitly prohibit the use of our services for illegal robocalling or deceptive caller ID spoofing.

3. Network Monitoring and Traffic Analysis

We employ automated and manual tools to identify suspicious calling patterns, including:

- **Volume Spikes:** Monitoring for sudden, large increases in call volume from a single source.
- **Call Completion Rates:** Analyzing low call-completion ratios and high volumes of short-duration calls (e.g., under 6 seconds).
- **Sequential Dialing:** Identifying patterns indicative of "wardialing" or sequential number attempts.
- **Fraud Detection:** Utilizing industry-standard fraud prevention tools to flag known bad actors or suspicious ANI (Automatic Number Identification) behavior.

4. STIR/SHAKEN Implementation Status

- **Implementation:** [Select one: We have fully implemented STIR/SHAKEN / We have partially implemented STIR/SHAKEN / We are currently exempt from implementation but follow this mitigation plan].
- **Attestation:** For traffic originating on our network, we apply the highest level of attestation possible based on our knowledge of the customer's right to use the telephone number.

5. Traceback Cooperation

[Your Company Name] commits to fully cooperating with the industry traceback consortium (the ITG), the FCC, and law enforcement.

- **Response Time:** We maintain a dedicated point of contact to respond to all traceback requests within **24 hours** of receipt.
- **Upstream Investigation:** We work with upstream providers to identify the source of any illegal traffic that transits our network.

6. Enforcement and Mitigation Actions

If a customer is found to be originating illegal robocalls, **[Your Company Name]** takes immediate action, which may include:

- Issuing a formal warning and requiring immediate cessation of the activity.
- Limiting or suspending the customer's ability to originate calls.
- Terminating the service agreement for cause.
- Reporting the activity to the FCC or relevant law enforcement authorities as required.

7. Annual Recertification and Updates

This plan is reviewed annually. In accordance with FCC rules, we will recertify this plan in the Robocall Mitigation Database by March 1st of each year, or within 10 business days of any significant change to our mitigation practices.