



Robocall Mitigation Program Description

Jabber Jaw Telecom maintains a Robocall Mitigation Program designed to prevent, identify, and respond to illegal or unwanted robocalling activity on its network. The program includes both proactive and reactive measures to mitigate potential misuse.

In the event of suspected fraudulent, unlawful, or abusive calling activity, Jabber Jaw Telecom takes immediate corrective action, which may include one or more of the following steps:

- **Change SIP Credentials:** Compromised SIP passwords are promptly reset to prevent unauthorized access to the network.
- **Change or Block Caller ID:** Caller ID values associated with suspicious activity are modified, restricted, or blocked to prevent spoofing or misuse.
- **Take Devices Offline:** Affected endpoints, IP phones, PBXs, or gateways may be temporarily taken offline to stop ongoing or potential robocall activity.
- **Delete or Disable Extensions:** Compromised or abused extensions are deleted or disabled until security can be verified and restored.
- **Carrier Escalation:** Incidents are reported to and coordinated with our upstream white-label carrier to investigate, mitigate, and prevent further abusive traffic.

Additionally, Jabber Jaw Telecom monitors traffic patterns for anomalies, enforces acceptable use policies, and cooperates fully with upstream providers and regulatory authorities as required. Customers found to be in violation of robocall regulations or company policy may face suspension or termination of service.

This mitigation program is reviewed and updated as necessary to ensure ongoing compliance with FCC robocall mitigation requirements.