

Robocall Mitigation Plan
Gigs Wireless Inc.

Gigs Wireless Inc. (“Company” or “Gigs”) submits the following Robocall Mitigation Plan in compliance with 47 CFR § 64.6305(d)(ii)-(iii).

Reasonable Steps to Prevent New and Existing Customers from Originating Illegal Calls:

Gigs has implemented meaningful protections to avoid originating illegal robocalls as part of its robocall mitigation program. For instance, Gigs customers must agree to its Terms & Conditions, including its Acceptable Use Policy. Customers agree that they not use the service for illegal or unlawful activities, to transmit inappropriate content, to infringe intellectual property rights of others, or to harm the service or Gigs’ network. Customers are also not permitted to use the services in any way that is inconsistent with personal use, and may not use them for any commercial purposes, including telemarketing, autodialing, public hotspots, tethering, hosting services, or never-ending call or data use sessions.

Gigs reserves the right to terminate any and all services if Gigs believes, in its sole discretion, that the customer has breached any obligation of the Terms & Conditions, including the Acceptable Use Policy.

Description of Analytics to Block Illegal Traffic:

Gigs’ strategy revolves around a meticulous methodology designed to pinpoint patterns typically associated with such activities. Gigs only uses custom-built in-house tools and does not use third-party services or vendors:

- **Identify High Frequency Callers/Texters:** We monitor for unusually high frequencies of calls or texts, which can be indicative of automated systems.
- **Diversification of Called Numbers:** We examine the diversity of numbers called or texted, as robocalls often target large volumes of contacts.
- **Short Duration Calls (Voice only):** We flag calls with exceptionally short durations, particularly those limited to voice communication, which are common characteristics of robocalls.
- **Ratio of Outgoing Calls/Texts by Number of Unique Numbers Called/Texted:** Robocalls typically exhibit a ratio closer to 1, indicating repetitive outreach to a limited number of recipients.
- **Fraudulent accounts suspension:** On top of monitoring activity gigs monitors activity and suspends in accordance with the ToS they sign upon purchase of the plan
- **Customer identification:** Gigs collects, name, address and device type upon sign up. Additionally we rely on fraud tools provided by our service providers to mitigate and prevent fraud on our connectivity services.

By collectively applying these criteria and thresholds to our data, we're able to flag potential robocalls or robotexts for further investigation. Each flagged line undergoes manual profiling to determine its nature.

In addition to our internal efforts, our partnership with Mobile Network Operators (MNOs) plays a crucial role in combating robocalls and robotexts. Here are some measures our MNO partners take:

1. **Implementing Caller Authentication:** Leveraging STIR/SHAKEN technology deployed by our MNO partners to authenticate caller IDs and verify the legitimacy of calls made through our network.
2. **Enhancing Call Blocking and Filtering:** Utilizing advanced call-blocking and filtering tools provided by our MNO partners to identify and block known scam numbers, spam calls, and robocalls before they reach our users' phones.
3. **Enforcing Robocall Mitigation Programs:** Collaborating with our MNO partners to enforce robust robocall mitigation programs, ensuring that all calls originating from our network comply with anti-spoofing standards and regulations.
4. **Utilizing Real-time Call Analysis:** Leveraging the real-time call analytics systems implemented by our MNO partners to detect suspicious calling patterns and behaviors, enabling prompt identification and prevention of fraudulent activity.
5. **Educational Initiatives:** Working alongside our MNO partners to launch educational campaigns aimed at raising awareness among our users about the risks of robocalls and empowering them to recognize and report fraudulent activity.
6. **Collaborating with Law Enforcement:** Partnering with our MNO counterparts to collaborate with law enforcement agencies in identifying and investigating illegal robocall operations, contributing to the prosecution of perpetrators.
7. **Implementing Network-level Blocking Solutions:** Utilizing network-level call blocking solutions provided by our MNO partners to automatically intercept and block calls identified as fraudulent or suspicious, enhancing our users' security.
8. **Establishing Feedback Loops:** Collaborating with our MNO partners to establish feedback loops with users to gather information on reported robocalls, allowing for continuous refinement of call-blocking algorithms and improvement in accuracy.
9. **International Cooperation:** Working closely with our MNO partners to collaborate with international telecommunications regulators and operators in addressing cross-border robocall scams and sharing information on emerging threats and best practices.
10. **Ensuring Regulatory Compliance:** Partnering with our MNOs to ensure compliance with regulatory requirements and standards, such as the FCC's mandates for call authentication and robocall mitigation, to maintain consumer trust and avoid penalties.

Additionally, our MNO partners offer specific features which include:

- Automatic Fraud Blocking detects and blocks calls from likely fraudsters.
- Suspected Spam Warning identifies telemarketers and other suspected spam calls.
- Personal Block List lets you block unwanted calls by number.
- Device security/breach report alerts.
- Advanced features such as Public Wi-Fi Protection, Identity Monitoring, Reverse Number Lookup, Safe Browsing, and Theft Alerts notify you if suspicious activity is detected (available on Android devices only).

Know Your Customer Practices:

Gigs collects, name, address and device type upon sign up. Additionally we rely on fraud tools provided by our service providers to mitigate and prevent fraud on our connectivity services.

Know Your Upstream Provider Practices:

Gigs' upstream providers are nationwide mobile network operators ("MNOs"). Gigs cooperates with its upstream MNOs and third parties, as necessary, to determine the origin of a voice call to or from a United States phone number that is suspected of being an illegal robocall.

Commitment to Respond to Traceback Requests:

Gigs is willing and able to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

This Robocall Mitigation Plan describes the specific measures that Gigs has implemented to as of 2026.02.26. Gigs continually evaluates the efficacy of its measures to combat bad actors and takes appropriate steps to improve these measures when needed.