

Gabbit, LLC
Robocall Mitigation Plan

Gabbit is committed to actively eliminating the ability of its customers to participate in any form of illegal activity.

Traffic Monitoring

Gabbit monitors calling activity using analytics to automatically flag and shutdown calling patterns indicative of robocalls, including both toll fraud and calling patterns that violate our Terms and Conditions. Our customers have a rate limit, and internal alarms are triggered if call limits are reached. Gabbit will block services to a customer if it determines that the customer is using the services for any illegal activities, including robocalling.

Gabbit has implemented the following policies and practices to prevent the origination of illegal robocalls and to quickly detect (and terminate) any customers found (or suspected) to be in violation:

1. Customers are only able to place calls originating from their own phone number. Caller ID and call records are reviewed when service is installed to verify legitimate caller ID Information.
2. All calls are generated by human interaction - Gabbit does not have any process to autogenerate calls.
3. Gabbit's firewalls permit traffic only from the customers' IP addresses.
4. Gabbit utilizes call blocking technology to automatically block known robocall numbers and suspicious calls identified by analytics.
5. All voice traffic originating from our network is continuously monitored using automated tools to detect the following: (a) unusual (or non-human) calling patterns; (b) high call volumes; and (c) traffic congestion or variations in call volume made from a particular customer or endpoint.
6. Gabbit immediately reacts to any complaints from upstream carriers by investigating and blocking calls from a customer found (or suspected) to be in violation.
7. Terminate services and delete accounts found to be fraudulent and/or in violation of Gabbit's use policies (as set forth in Gabbit's Terms and Conditions).

Customer Vetting

All customers are subject to a strict onboarding process. This includes verifying business identity, understanding the intended use of our services, and ensuring compliance with FCC rules and applicable laws. Gabbit requires all users of its services to comply with applicable laws

prohibiting illegal robocalling and providing for blocking or termination of services for those that breach such provisions.

Gabbit's contracts and Terms and Conditions currently prohibit the use of Gabbit services to engage in fraudulent or illegal activity, reserving Gabbit's right to refuse service and terminate the contract if the customer does engage in such conduct. Gabbit actively enforces these contractual provisions. As a normal course of business operations, Gabbit routinely reviews its contracts and makes necessary modifications.

Outbound Calling and Call Authentication Practices

Gabbit exclusively uses Intelliquent for all outbound calling and phone number provisioning. By consolidating these services with Intelliquent, all calls originating from Intelliquent-provided phone numbers are signed with full STIR/SHAKEN "A" attestation, ensuring compliance, and reducing the likelihood of call blocking by terminating carriers. Intelliquent uses software to monitor outbound voice traffic in real time and provides detailed reporting identifying if our network originates any calls where the calling number is invalid, unallocated, on a Do Not Originate list, in the FCC consumer complaint database or has a poor reputation. Gabbit receives real-time notifications about telephone numbers originating suspected illegal robocalls on its network. The software's identification of suspected illegal robocalls and alerts helps prevent the origination of illegal robocalls.

Calls are signed with appropriate certificates to validate the originating number. Any non-IP-based calls or calls that cannot be authenticated using STIR/SHAKEN are subject to alternative mitigation measures, such as real-time traffic analysis and additional scrutiny.

Our support team is trained to address customer concerns, investigate reports of suspected robocalls, and assist clients in mitigating abuse of their accounts.

Compliance with Government Agencies

Gabbit is committed to responding to all traceback requests from law enforcement and the industry traceback consortium. We respond promptly to aid in identifying and stopping any illegal robocalling activities originating from our network. In addition, Gabbit will cooperate with such entities to investigate and stop any illegal robocalls that use its service to originate calls. All of the voice traffic that originates on our network is subject to a robocall mitigation program. Gabbit certifies these specific and reasonable steps have been taken to avoid originating illegal robocall traffic as part of its robocall mitigation program.

Robocall Mitigation Database Eligibility

Neither Gabbit or any affiliated entity has been involved in any law enforcement or regulatory investigation into suspected unlawful robocalling in the prior two years. Gabbit has not been prohibited from filing in the Robocall Mitigation Database.

Certification and Commitment

Gabbit certifies that it has implemented the practices outlined in this document and will comply with all applicable FCC rules and regulations.

Conclusion

By leveraging Intelliquent's robust STIR/SHAKEN capabilities and implementing stringent internal monitoring and mitigation practices, Gabbit ensures compliance with industry standards and actively works to prevent illegal robocalls.

If you have any questions please contact Gabbit at:

Gabbit, LLC

9415 Dielman Rock Island Industrial Drive

St. Louis, MO 63132

Attention: Harry Orchard, CEO

314-898-0000

harry@gabbit.com

Submitted: December 20, 2024

Gabbit, LLC