

At Kallstar, we take fraud prevention and security seriously to maintain the integrity of our VoIP routes. We have implemented a multi-layered approach to detect, prevent, and mitigate fraudulent activities, ensuring compliance with regulatory requirements and safeguarding our network and clients.

1. Real-Time Traffic Monitoring

We utilize advanced AI-driven analytics and real-time monitoring tools to detect unusual call patterns, including:

- High call volume spikes from a single source.
- Short-duration calls with high frequency.
- Calls to high-risk destinations or premium-rate numbers.
- Unauthorized attempts to access our VoIP infrastructure.

2. Blacklisting and Whitelisting Mechanisms

We maintain and regularly update:

- A **blacklist** of known fraudulent IPs, numbers, and traffic sources to automatically block suspicious activity.
- A **whitelist** of verified users, ensuring only authorized traffic is permitted through our VoIP network.

3. Caller ID and ANI Validation

To prevent spoofing and fraudulent call masking, we implement:

- **Caller ID authentication** using STIR/SHAKEN protocols to validate the legitimacy of incoming calls.
- **Automatic Number Identification (ANI) validation** to verify the authenticity of originating numbers.

4. Geo-Fencing and IP Restrictions

We prevent unauthorized access by:

- Restricting VoIP traffic to approved geographic regions.
- Blocking calls originating from high-risk or unapproved locations.
- Implementing IP-based authentication to allow only trusted sources to access our routes.

5. Rate-Limiting and Call Capping

To prevent fraudulent bulk traffic, we enforce:

- **Rate-limiting** on call attempts per second (CPS) to detect and stop automated fraudulent calls.
- **Call capping** for certain destinations to limit excessive call traffic.

6. Fraud Detection Algorithms & AI-Based Filtering

Our AI-based filtering system detects:

- Call behavior anomalies that indicate possible fraud.
- Robocall and spam traffic patterns.
- Abnormal call durations that deviate from typical user behavior.

7. Compliance with Regulatory Standards

We adhere to industry regulations, including:

- **FCC (Federal Communications Commission) and FTC (Federal Trade Commission) guidelines** for VoIP traffic.
- **TCPA (Telephone Consumer Protection Act) compliance** to avoid unauthorized telemarketing calls.
- **GDPR and data privacy laws** to protect user information from misuse.

8. Customer Authentication & Access Control

To prevent unauthorized usage:

- Customers must complete **multi-factor authentication (MFA)** before accessing VoIP services.
- We enforce strict **password policies and encryption** to protect SIP credentials.

9. Regular Audits and Security Updates

- We conduct **regular security audits** to identify vulnerabilities in our VoIP infrastructure.
- Continuous **firmware and software updates** are applied to mitigate known threats.

10. Collaboration with Industry & Law Enforcement

- We work with **anti-fraud consortiums** to exchange intelligence on scam tactics.
- We promptly report fraud cases to **law enforcement and telecom regulators**.

Through these proactive measures, Kallstar ensure a **secure, reliable, and fraud-free VoIP environment**, protecting both our clients and end-users from malicious activity.

As a voice service provider, we are committed to implementing a robust and compliant robocall mitigation program in accordance with the requirements set forth by the FCC under 47 CFR § 64.1200.

Our robocall mitigation program includes the following measures:

1. **Reasonable Steps to Prevent Illegal Robocall Traffic**

We employ advanced traffic monitoring tools and maintain strict Know-Your-Customer (KYC) onboarding procedures to verify the identity and legitimacy of all customers. Our systems are configured to detect anomalous call patterns and high-risk traffic behaviors. Any suspicious activity is immediately investigated, and appropriate action is taken to suspend or terminate offending traffic.

2. **Customer Vetting and Monitoring**

All customers undergo a comprehensive vetting process prior to onboarding. This includes identity verification, business validation, and usage intent checks. We continuously monitor traffic patterns and enforce usage policies to prevent misuse of our platform.

3. **Cooperation with Authorities**

We fully cooperate with the Commission, law enforcement agencies, and the industry traceback consortium in efforts to combat illegal robocalls.

4. **Commitment to Timely Traceback Response**

We commit 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 our service to originate, carry, or process calls.

Contact Us: For any security concerns or to report suspicious activity, please contact our **Fraud Prevention Team** at fraud@kallstar.com .