

Robocall Mitigation Program Description CNETGEEK

CNETGEEK has implemented a comprehensive robocall mitigation program designed to prevent the origination of illegal robocalls on our network.

1. **Know-Your-Customer (KYC):**

Verification We perform business identity verification on all customers before enabling voice services. This includes validating company ownership, service use case, contact information, and intended traffic profile. High risk customers are rejected or require enhanced due diligence.

2. **STIR/SHAKEN:**

Implementation All eligible SIP calls are signed with STIR/SHAKEN through our upstream carriers. We ensure authenticated caller ID and support validation of inbound calls.

3. **Traffic Monitoring & Fraud Detection:**

We continuously monitor outbound call traffic for indicators of unlawful robocalling, including high volume short duration patterns, invalid caller IDs, sudden traffic spikes, and known fraud signatures.

4. **Call Blocking & Rate Limiting Controls:**

Automated systems enforce call throttling, destination restrictions, and fraud pattern blocking. Customers generating prohibited traffic are rate limited or immediately suspended.

5. **Rapid Traceback Response:**

We fully cooperate with the Industry Traceback Group (ITG) and respond promptly to traceback requests. Detailed logs are maintained to support investigations.

6. **Customer Enforcement Policy:**

If a customer is identified as originating unlawful robocalls, we take immediate corrective action including warnings, call blocking, suspension, or account termination.

7. **Ongoing Compliance & Review:**

Our engineering and compliance teams regularly review mitigation performance, update procedures, and ensure continuous alignment with FCC requirements. CNETGEEK is committed to preventing illegal robocalls and maintaining full FCC compliance

CNETGEEK prohibits any unlawful, abusive, or fraudulent use of our voice services.

Customers may not originate illegal robocalls, spoof caller ID without authorization, engage in high-risk or fraudulent calling behavior, or violate Do-Not-Call (DNC) regulations.

We monitor outbound traffic for indicators of abuse including unusual call spikes, high-volume short-duration calls, invalid caller ID usage, and known fraud patterns. Suspicious activity may result in immediate call blocking, rate limiting, account suspension, or termination without notice. Customers are responsible for secure use of their PBX or SIP devices and must comply with all FCC rules and traceback investigations. CNETGEEK may update this policy at any time to address new risks or regulatory requirements.