

Cnet System Robocall Mitigation Plan

Comprehensive Measures for Preventing Illegal Robocall Traffic

Introduction

Cnet System is committed to maintaining the highest standards of integrity and compliance in all facets of its voice communications business. As a provider leveraging CoreDial's VOIP infrastructure, Cnet System recognizes its responsibility to prevent the origination, carrying, or processing of illegal robocall traffic. This robocall mitigation plan outlines the specific, reasonable steps Cnet System is taking as part of its comprehensive robocall mitigation program, tailored to the roles it serves within the call chain. The following sections detail affirmative measures for customer onboarding, analytic systems in use, and procedures for understanding upstream provider relationships.

1. Affirmative, Effective Measures to Prevent New and Renewing Customers from Originating Illegal Robocalls

Customer Vetting and Onboarding Process

Cnet System implements a rigorous customer vetting process before onboarding any new customer or renewing business relationships. The process includes:

- **Know Your Customer (KYC) Protocols:** All new and renewing customers must provide comprehensive identification, business registration documents, and verification of legal status.
- **Risk Assessment Questionnaires:** Prospective customers are required to complete detailed questionnaires focused on intended call volumes, call patterns, and business models to identify potential for robocall activity.
- **Screening for High-Risk Profiles:** Cnet System applies enhanced scrutiny to customers operating in industries historically associated with higher robocall volumes (e.g., marketing, debt collection, telemarketing). Such customers may be subject to additional documentation requests, interviews, or even denial of service.
- **Agreement to Acceptable Use Policies:** All customers must agree to Cnet System's Acceptable Use Policy (AUP), which strictly prohibits the origination, transmission, or facilitation of illegal robocalls. Violations trigger immediate investigation and potential termination of service.

Ongoing Monitoring and Renewal Checks

- **Periodic Account Audits:** Cnet System conducts scheduled reviews of active customer accounts, focusing on patterns in call traffic, changes in usage profiles, and adherence to the AUP.
- **Renewal Screening:** Before renewing any customer contract, Cnet System re-examines call histories and business practices. Any indications of illegal robocall activity result in denial of renewal, further investigation, or reporting to relevant authorities.
- **Education and Compliance Training:** Cnet System provides ongoing education to its customers about legal requirements and best practices for telecommunication traffic. Customers are updated regularly on new regulatory developments, ensuring compliance awareness is maintained.

Rapid Response to Suspected Robocall Activity

- **Immediate Suspension Protocols:** If illegal robocall activity is suspected, Cnet System immediately suspends the customer account pending investigation. Where clear violations are found, services are terminated, and relevant authorities are notified.
- **Collaborative Remediation:** For minor or inadvertent incidents, Cnet System works with customers to remediate issues, educate them on compliance, and monitor for future violations.

2. Call Analytic Systems Utilized by Cnet System

Cnet System uses CoreDial's robust VOIP infrastructure, which incorporates industry-leading call analytic systems for detecting and mitigating illegal robocall traffic.

CoreDial's Call Analytics Overview

- **Automated Call Pattern Analysis:** CoreDial's platform continuously monitors call traffic for suspicious patterns indicative of robocall campaigns, such as high-volume short-duration calls, sequential dialing, and calls to unallocated or invalid numbers.
- **Real-Time Call Blocking:** When CoreDial's systems detect probable illegal robocall activity, they automatically block or flag calls for further review, reducing the likelihood that such calls reach end users.

- **Integration with Industry Databases:** CoreDial leverages third-party databases and government-provided resources (e.g., FCC, STIR/SHAKEN) to cross-reference call signatures and known illegal robocall sources.
- **STIR/SHAKEN Compliance:** CoreDial's infrastructure is compliant with the STIR/SHAKEN framework, providing call authentication and attestation mechanisms that help ensure the legitimacy of caller IDs.
- **Third-Party Vendor Partnerships:** CoreDial partners with recognized analytic vendors to provide additional layers of protection, including advanced fraud detection algorithms and real-time threat intelligence feeds.

Internal Monitoring and Reporting

- **Dashboard Access:** Cnet System maintains direct access to analytic dashboards provided by CoreDial, enabling real-time monitoring of call traffic and alerting to suspicious activities.
- **Automated Alerts:** The system generates automatic alerts for potentially illegal robocall events, allowing Cnet System staff to intervene promptly.
- **Trend Analysis and Reporting:** Regular reports are generated to identify emerging trends in call traffic and to document steps taken to mitigate any detected illegal activity.

3. Procedures for Knowing Upstream Providers

Upstream Provider Verification and Collaboration

As a customer of CoreDial, Cnet System's upstream provider is singularly CoreDial for all VOIP traffic. Cnet System applies the following procedures:

- **Due Diligence Review:** Prior to contracting with CoreDial, Cnet System conducted a thorough due diligence review of CoreDial's robocall mitigation policies, STIR/SHAKEN compliance, call analytics systems, and reputation in the industry.
- **Continuous Relationship Assessment:** Cnet System maintains open communication channels with CoreDial, regularly reviewing service agreements, compliance updates, and technical enhancements related to robocall mitigation.
- **Documentation and Audit:** Cnet System keeps records of CoreDial's certifications, compliance reports, and periodic audits to ensure ongoing adherence to regulatory requirements and best practices.
- **Incident Response Coordination:** In the event of detected illegal robocall activity, Cnet System collaborates directly with CoreDial's technical and compliance teams to investigate, remediate, and report incidents as necessary.

- Industry Engagement: Cnet System participates in industry forums and working groups with CoreDial, staying abreast of developments in robocall mitigation technology and regulation.

Application of CoreDial's Robocall Mitigation Programs to Cnet System

Because Cnet System utilizes CoreDial's VOIP infrastructure, all robocall mitigation measures, analytic systems, and compliance frameworks employed by CoreDial are fully extended to Cnet System's voice traffic. This includes:

- Call Authentication: All calls carried by Cnet System are subject to STIR/SHAKEN authentication mechanisms operated by CoreDial, helping prevent caller ID spoofing and ensuring call legitimacy.
- Traffic Analytics: CoreDial's call analytic engines continuously monitor Cnet System's call traffic for anomalies, with real-time blocking and alerting features active on all inbound and outbound calls.
- Regulatory Compliance: CoreDial's compliance team works in tandem with Cnet System to ensure adherence to FCC and industry mandates for robocall mitigation.
- Reporting and Transparency: Cnet System receives regular reports from CoreDial detailing analytic results, blocked call statistics, incidents of suspected illegal robocall activity, and actions taken.

Conclusion

Cnet System's robocall mitigation program is designed to address the risks of illegal robocall origination, carriage, and processing at every critical point in the call chain. By leveraging CoreDial's advanced infrastructure and analytic tools, Cnet System implements affirmative and effective measures to rigorously vet customers, monitor call traffic, and maintain robust relationships with its upstream provider. These efforts collectively ensure that Cnet System remains compliant with regulatory requirements and is an active participant in the industry-wide fight against illegal robocall traffic.

Cnet System will continue to refine its mitigation plan as new threats, regulations, and technologies emerge, remaining vigilant in its mission to provide secure, reliable, and compliant voice communications services.