

Robocall Mitigation Plan

Filer Information:

Company Name: Konceptio Data Services, LLC DbA KDS Networks, KDS Fiber

Type of Provider: Internet Service Provider (ISP) offering resold VoIP services

Service Area: Cascade County, Montana

Introduction:

Konceptio Data Services, LLC provides broadband and VoIP voice services to end-users by reselling services from Ooma, Blackfoot Communications, Inc., 9171-5573 Quebec Inc. (Voip.ms), and BRCK (formerly Bandwidth). We recognize our responsibility to help mitigate illegal and unwanted robocalls on our network. In compliance with Federal Communications Commission (FCC) rules, Konceptio Data Services, LLC has developed this Robocall Mitigation Plan to detail our efforts to prevent the origination and transmission of unlawful robocalls.

1. STIR/SHAKEN Implementation

Konceptio Data Services, LLC certifies that it is working closely with its underlying voice service providers to ensure compliance with STIR/SHAKEN call authentication standards as required by 47 CFR § 64.6301. Since we rely on our wholesale partners' infrastructure, we are coordinating with them to ensure that:

- All IP-based calls that can support STIR/SHAKEN are properly signed with an authentication attestation level reflecting the caller's identity verification status.
 - Calls are passed along with STIR/SHAKEN identity headers intact, ensuring that downstream providers and terminating carriers can verify call authenticity.
-

2. Customer Vetting and Monitoring

We implement the following measures to ensure that customers using our voice services are legitimate and do not engage in illegal robocalling:

- **Customer Identity Verification:** We verify the identity of new customers through standard account setup procedures, including verification of business identity (if applicable).
- **Acceptable Use Policies:** Our terms of service prohibit illegal robocalls and other harmful calling practices. Violators may have their accounts suspended or terminated.
- **Traffic Pattern Monitoring:** We monitor call records for abnormal patterns (e.g., sudden surges in short-duration calls) that may indicate illegal robocall activity. Suspicious activity triggers additional review and possible enforcement actions.

3. Network and Device Security

Ensuring the security of the network environment and VoIP infrastructure is critical to preventing unauthorized usage that could facilitate illegal robocalls. We:

- **Open VoIP Device Scanning:** Regularly scan and monitor our network for unsecured or “open” VoIP endpoints. Any identified vulnerabilities are promptly addressed.
- **Device Management and Patching:** Devices managed by Konceptio Data Services, LLC are continuously monitored, and we promptly apply the latest security patches and firmware updates. This ensures unauthorized access or exploitation of VoIP devices is minimized.
- **Access Controls:** We maintain strict access control policies, strong authentication mechanisms, and routine security audits to prevent unauthorized access to any VoIP device or management system.

4. Upstream Provider Collaboration and Monitoring

Since Konceptio Data Services, LLC relies on upstream VoIP providers (Ooma, Blackfoot Communications, Voip.ms, and BRCK), we maintain open communication and contractual obligations to ensure compliance with robocall mitigation strategies:

- **Require Compliance:** We only work with providers who attest to STIR/SHAKEN compliance or have equivalent mitigation measures in place.
- **Audits and Reviews:** We periodically review our upstream providers’ certifications, compliance statements, and ongoing mitigation efforts.
- **Escalation Processes:** If suspicious call patterns appear to originate from upstream suppliers, we report these issues and work with them to take corrective action, including blocking or filtering bad actors.

5. Call Analytics and Blocking Tools

Konceptio Data Services, LLC uses industry-standard call analytics tools (or those provided by our upstream partners) to identify potentially fraudulent or illegal robocall traffic:

- **Reputation-Based Blocking:** Employ scoring mechanisms to identify known scam call patterns and block them before reaching end-users.
 - **Alerts and Thresholds:** Establish thresholds for call volumes and attempt velocities; exceeding these triggers alerts for further scrutiny.
 - **Continuous Improvement:** Review call detail records and analytics reports to refine blocking thresholds and improve detection criteria over time.
-

6. Transparency and End-User Education

We believe educating our customers is crucial in combating illegal robocalls:

- **Guidance Resources:** Provide tips and resources on recognizing scam calls, avoiding unknown numbers, and reporting suspicious calls to authorities.
 - **Feedback Loop:** Encourage customers to report suspicious or unwanted calls, helping us refine our mitigation strategies.
-

7. Ongoing Compliance and Improvement

Robocall mitigation is an evolving challenge, and we are committed to ongoing enhancement:

- **Staying Informed:** Keep up-to-date on FCC rules, industry best practices, and technological improvements.
 - **Periodic Internal Reviews:** Regularly assess our mitigation program's effectiveness and update policies and procedures as needed.
 - **Industry Collaboration:** Participate, where possible, in industry forums and best practice groups to share insights and strengthen collective efforts against illegal robocalls.
-

Conclusion

Konceptio Data Services, LLC is dedicated to robust robocall mitigation practices, including implementing STIR/SHAKEN, monitoring network security, vetting customers, leveraging analytics, and collaborating with upstream providers. Through these comprehensive strategies, we strive to minimize the occurrence of illegal and unwanted robocalls, thereby enhancing the trust and reliability of our voice services.