

Robocall Remediation Plan

Business Information

- **Legal Business Name:** Digital Security Services, Inc. DBA DP Tech Group
- **Business Address:** 2198 Gladstone Ct. Suite A. Glendale Heights, IL. 60139
- **Primary Contact Information:** Raj Lamba, President
 - **Contact Email:** rlamba@dptechgroup.com
 - **Contact Phone Number:** 630-372-0100 x 103
- **RMD File Number:** 0031377799

Traceback Response Commitment

DP Tech Group fully commits to responding requests from the FCC, law enforcement, or the registered traceback consortium within 24 hours. DP Tech Group shall actively cooperate with these entities to investigate and cease any illegal robocalling activity utilizing the Company's service.

- **Designated Contact:** Raj Lamba, President email: rlamba@dptechgroup.com phone: 630-372-0100 x103
- **Collaboration with Upstream Providers:** We work closely with our upstream providers to access call records and ensure accurate and timely responses.

Know Your Customer (KYC) Practices

Our rigorous customer verification process, combined with our focus on serving primarily local, established businesses, effectively minimizes the risk of misuse for generating robocalls.

Face-to-Face Verification

We exclusively provide services for small businesses and do not serve individual consumers. To ensure the legitimacy of our clients, we meet all customers in person to establish their identity and validate their business operations. Additionally, we conduct interviews to understand their calling needs, strictly prohibiting any form of automated or unauthorized calling, including auto-dialers, predictive dialers, or other call-center-type systems.

Customer Education

- We educate our customers about our strict policies that prohibit robocalls, high-volume calling, and the use of automated call systems.

Robocall Mitigation Program

We have implemented the following steps to prevent unauthorized robocalls:

Restricted Customer Connectivity to Approved Devices

Customers are not allowed to set up their own VoIP equipment. All hardware is exclusively approved, configured, and managed by our technical support team, with no access provided to connection credentials. This ensures only authorized devices can make VoIP calls, preventing unauthorized servers or devices from being added for robocalls.

Multi-Layered Call Traffic Monitoring & Blocking

- All call traffic originating from our systems is actively monitored through our VoIP server and upstream providers.
- Monitoring includes tracking call volume, duration, and patterns to identify and mitigate suspicious activity.
- Our upstream providers enforce high standards with strict guidelines and requirements to prevent unauthorized robocalls.
- Suspicious activity, such as unusually high call volumes or short-duration calls indicative of robocall activity, is promptly flagged and blocked.

Account Suspension and Notification

- When suspicious activity is detected, our upstream provider immediately blocks the calls and suspends the account associated with the activity.
- Notifications are promptly sent to our team for further review and investigation.

Use of Call Analytics Systems

- **Comprehensive CDR Logs:** We capture and store detailed data for all calls, including origin, destination, timestamps, duration, and call disposition, ensuring full traceability directly on our VoIP server.
- **Pattern Analysis:** We use this data to identify patterns or suspicious activity for detecting and mitigating robocalls.
- **Proactive Actions:** Our upstream providers utilize real-time call monitoring, anomaly detection, and proactive call blocking based on risk analysis to stop unauthorized calls.

Recordkeeping Practices

- **Call Log Retention:** We securely store comprehensive call detail records (CDRs), including origin, destination, timestamps, duration, and call disposition, for a minimum of 12 months.
- **Traceback Support:** Records are readily accessible to support traceback investigations and compliance audits.
- **Secure Storage:** All records are stored in a secure environment to ensure data integrity and prevent unauthorized access.

Employee Training and Internal Audits

- **Employee Training:** Staff members receive regular training on robocall mitigation practices, compliance requirements, and traceback protocols.
- **Internal Audits:** We conduct periodic reviews of our systems and processes to ensure adherence to the Robocall Mitigation Plan and identify areas for improvement.

Plan Review and Updates

- **Regular Reviews:** The Robocall Mitigation Plan is reviewed annually or whenever FCC requirements change.
- **Continuous Improvement:** Feedback from audits, investigations, and industry developments is incorporated into updates to ensure compliance and effectiveness.
- **Public Accessibility:** A summary of our Robocall Mitigation Plan is available to stakeholders upon request to promote transparency.

Reporting and Notification

- **Incident Reporting:** Any suspected robocall activity is promptly reported to the FCC or law enforcement as required.
- **Collaboration with Upstream Providers:** We coordinate with upstream providers to ensure timely and accurate reporting of suspicious activities.
- **Audit Trail:** All significant actions, including account suspensions and traceback responses, are logged and maintained as part of an audit trail for accountability.

Security Measures Against Fraudulent / Unauthorized Access

Fraudulent Robocalls

- Our upstream providers have implemented advanced fraud detection controls that align with industry's best practices and regulatory requirements. Combined with the comprehensive security measures established in our own Robocall Mitigation Plan, we are confident that these safeguards effectively detect and block fraudulent calls.

Brute Force Attack Prevention

- We have implemented mechanisms to ban and block endpoints that exceed a set threshold of failed login attempts through the use of a firewall.

IP Whitelisting and Geofencing

- Only authorized IP addresses and authenticated devices can connect to our VoIP server system to make phone calls.

STIR/SHAKEN Implementation

Call Authentication and Attestation

- We currently do not own or control the infrastructure to directly implement STIR/SHAKEN. Instead, we rely on the STIR/SHAKEN implementation provided by our upstream providers, which are reputable, well-established companies owned by publicly traded parent organizations.
- All outbound calls from our system are authenticated and assigned the appropriate attestation level by our upstream providers.
- Calls with A-level attestation are fully verified, indicating both the origin of the call and the legitimacy of the calling number.

Handling of Partial or Lower Attestation Calls

- Calls receiving B or C-level attestation are flagged for additional scrutiny to ensure compliance with robocall mitigation standards.

- Non-authenticated or low-attestation calls are either blocked or routed with clear labeling to identify their status.

Commitment to Compliance

- We ensure our systems are configured to support STIR/SHAKEN protocols with the assistance of our upstream providers, who maintain the necessary hardware and infrastructure. Together, we stay updated on advancements in call authentication technology and continuously review and enhance our processes to comply with evolving regulatory requirements.

Handling of Non-Authenticated Calls by Upstream Providers

- We have strong security controls in place to prevent non-authenticated calls from originating through our system, which is configured to allow access only from authorized devices maintained directly by our support team.
- In the event that non-authenticated calls are generated through our system, they are flagged by our upstream providers and subjected to enhanced scrutiny. Such calls are either blocked or routed with a lower attestation level to ensure transparency.
- Our upstream providers work with us to investigate any issues and take necessary corrective action to prevent misuse.

Know Your Upstream Vendor

DP Tech Group partners with Vitelity and VoIP Innovations to deliver VoIP services using their infrastructure. Our providers are reputable, well-established companies owned by publicly traded organizations. They have assured compliance with FCC STIR/SHAKEN and robocall mitigation rules, signing all calls originated by DP Tech Group. Both parties will actively collaborate to combat illegal robocalls and fully cooperate with traceback requests.

Contact info for upstream providers

Provider Information

- **Name of Provider:** VOIP Innovations (VI Communication Services, VoIPStreet)
- **Nature of Business:** Voice Services
- **Address:** One Penn Center West Suite 400, Pittsburgh PA 15276
- **Phone Number:** 412-326-3019

Provider Information

- **Name of Provider:** ANPI, LLC (Vitelity & Inteliquent)
- **Nature of Business:** Voice Services
- **Address:** 550 W Adams Street Suite 900, Chicago, IL. 60661
- **Phone Number:** 303-997-2300
- **Email:** Support@vitelity.net

Compliance Statement

This Robocall Mitigation Plan underscores DP Tech Group's unwavering commitment to preventing illegal robocalls and ensuring full compliance with FCC regulations. We remain dedicated to regularly reviewing, updating, and enhancing our practices to align with evolving regulatory requirements and industry best practices.

Traceback Point of Contact

Name: Raj Lamba

Title: President

Phone: 630-372-0100 x103

Email: rlamba@dptechgroup.com

Date: 02/28/2026