

Voip-IT Services, Inc.

Know Your Customer (KYC) Plan

Robocall Mitigation Program — FCC Robocall Mitigation Database Filing

1. Overview and Purpose

Voip-IT Services, Inc. ("the Company") has established this Know Your Customer (KYC) Plan as part of its Robocall Mitigation Program in compliance with the Federal Communications Commission's rules and requirements under the Robocall Mitigation Database (RMD). This plan describes the Company's procedures for verifying customer identity and intended use, monitoring call traffic using both internal processes and a third-party analytics vendor, and taking action against customers who originate illegal robocall traffic.

2. New Customer Onboarding and Vetting

Before activating service for any new customer, the Company conducts a manual review and approval process. No new account is activated without completing the following steps:

- **Review of Intended Use Case:** Each prospective customer is required to describe their anticipated calling activities, including the nature of calls to be made (e.g., business notifications, customer service, sales), expected call volume, and target audience. The Company evaluates whether the described use is consistent with lawful calling practices.
- **Manual Review and Approval:** All new customer applications are reviewed by Company personnel prior to service activation. The review evaluates the customer's stated purpose, business type, and any red flags that may indicate a risk of illegal robocall traffic. Service is not provisioned until this review is complete and the application is approved.
- **Customer Agreement:** All customers are required to agree to the Company's Terms of Service, which prohibit the use of the Company's network for illegal robocalls, spoofed calls, or any calling activity that violates federal or state law, including the Telephone Consumer Protection Act (TCPA).

3. Third-Party Analytics Vendor: Bulk Solutions (BulkVS)

The Company uses Bulk Solutions (operating as BulkVS) as its third-party vendor for robocall analytics and traffic monitoring. Bulk Solutions provides the following services that directly support the Company's robocall mitigation efforts:

- **Robocall Scoring:** Bulk Solutions assesses each call using a scoring model trained on over 100 billion carrier calls annually, providing a constantly refreshed view of the probability that a given number is being used for robocalling.

- **STIR/SHAKEN Integration:** Transaction Detail Records (TDRs) from STIR/SHAKEN are incorporated as an additional data source in Bulk Solutions' scoring model.
- **Behavioral Pattern Detection:** The platform identifies behavioral attributes associated with robocalling, including neighbor spoofing events and sudden spikes in call volume.
- **Do-Not-Originate (DNO) Monitoring:** Numbers appearing on DNO lists sourced from industry organizations (e.g., USTelecom) and enterprises are flagged automatically.
- **Real-Time Alerts:** When suspected robocalling patterns are detected on the Company's network, Bulk Solutions sends near real-time alerts, enabling the Company to manually block the telephone number and notify terminating parties via CNAM overlay (e.g., 'ROBOCALLER').
- **Origination and Termination Protection:** The platform supports real-time queries for both outbound calls originating on the Company's network and inbound calls terminating to subscribers, allowing the Company to block or flag suspected robocalls at both ends.
- **Automatic Call Volume Limiting:** Bulk Solutions automatically drops calls that originate an unusually high number of simultaneous calls in a short period of time. This automated safeguard prevents burst-dialing patterns commonly associated with illegal robocall campaigns from passing through the Company's network, providing an additional layer of protection beyond manual monitoring and alerting.

4. Monitoring of Existing Customers

The Company applies its KYC procedures on an ongoing basis to existing customers, not solely at the time of onboarding. The following monitoring measures are in place for current customers:

- **Call Detail Record (CDR) Review:** The Company periodically reviews call detail records to identify unusual patterns, including abnormally high call volumes, high rates of unanswered or short-duration calls, or calling patterns inconsistent with a customer's stated use case.
- **Bulk Solutions Ongoing Monitoring:** The Company's third-party vendor, Bulk Solutions, continuously monitors traffic originating from the Company's network on behalf of the Company. Alerts generated by Bulk Solutions regarding existing customer accounts are reviewed and acted upon promptly.
- **Complaint Monitoring:** The Company monitors reports of complaints related to unwanted or illegal calls. Any complaint associated with an existing customer account is flagged for review.
- **Carrier Alerts:** The Company receives and acts upon alerts and notifications from its upstream carrier partners regarding suspected illegal traffic originating from its network. Such alerts are treated as a high-priority trigger for review of the associated customer account.

5. Reasonable Steps to Mitigate Illegal Traffic

When a customer account is identified as a potential source of illegal robocall traffic — whether through Bulk Solutions alerts, CDR review, complaint reports, or carrier notifications — the Company takes the following steps:

- **Initial Warning:** Upon first identification of suspicious or non-compliant activity, the Company issues a formal written warning to the customer, notifying them that their traffic patterns have been flagged and that continued non-compliant activity will result in suspension or termination of service.
- **Investigation:** The Company conducts an internal review of the customer's CDRs, stated use case, Bulk Solutions alert data, and any complaint or carrier notification data to determine whether a violation has occurred.
- **Suspension or Termination:** If the investigation confirms that the customer is originating illegal robocall traffic, or if the customer fails to remediate flagged activity following a warning, the Company will suspend or terminate the customer's service.
- **Cooperation with Authorities:** The Company cooperates fully with traceback requests from the USTelecom Industry Traceback Group, law enforcement agencies, and the FCC Enforcement Bureau. Upon receipt of a traceback request, the Company will promptly identify the originating customer and provide all responsive information.

6. Recordkeeping

The Company maintains records of its customer onboarding reviews, monitoring activities, Bulk Solutions alerts received and acted upon, warnings issued, and any actions taken against customers for robocall-related violations. These records are retained in accordance with applicable FCC rules and are available for production upon request by the Commission or law enforcement.

7. Plan Review and Updates

The Company reviews this KYC Plan on a periodic basis and updates it as necessary to reflect changes in the Company's operations, developments in FCC rules and guidance, and best practices in robocall mitigation. Any material changes to this plan will be reflected in the Company's updated RMD filing.

Voip-IT Services, Inc.

Jacob Hass

CEO

03/05/2026