

Robocall Mitigation Plan

Business Information Solutions Inc. submits this Robocall Mitigation Plan in compliance with FCC Order EB-TCD-25-000385901 and the requirements of the Robocall Mitigation Database (RMD). This plan describes our implementation of STIR/SHAKEN caller ID authentication, Know-Your-Customer procedures, traffic monitoring and analytics, remediation and blocking protocols, traceback cooperation, reseller controls, and governance practices.

Company Information

Legal Name: Business Information Solutions

FRN: 0037437803

Role(s): Voice Service Provider

1) STIR/SHAKEN Implementation & Attestation

We assign 'A' attestation when we have verified both the identity of the caller and their right to use the originating telephone number.

We assign 'B' attestation when we have verified customer identity but cannot verify TN association.

We assign 'C' attestation for gateway traffic where caller identity and TN association cannot be validated."

2) Know-Your-Customer (KYC) & Vetting

Business Information Solutions Inc. conducts thorough KYC checks before activating any customer for outbound voice service. We:

Verify corporate registration, EIN, and responsible party identification.

Confirm billing and service addresses against public/business records.

Require LOAs or other evidence of right-to-use assigned telephone numbers.

Collect descriptions of call use-cases, campaign type, expected volumes, and target geographies.

Apply enhanced due diligence to high-risk verticals (telemarketing, debt collection, lead-generation).

During service, we baseline customer traffic patterns and employ analytics to detect deviations. Customers whose traffic triggers alerts are reviewed manually.

Upon credible notice of illegal robocalling (FCC, traceback, or analytics), we suspend the affected traffic immediately, notify the customer, and require proof of remediation. Repeat or unremediated violations result in service termination.

3) Traffic Monitoring & Analytics

Business Information Solutions Inc. continuously monitors call traffic for patterns consistent with illegal or unwanted robocalls. We:

Establish baselines for each customer's expected call behavior (calls per second, average call duration, answer rates, and destination mix).

Proactively block traffic to invalid or unallocated NANP numbers, known Do-Not-Originate (DNO) ranges, and malformed SIP headers.

Employ analytics to detect anomalies such as sudden volume spikes, high concentrations of short-duration calls, or disproportionate traffic to specific destinations.

Generate real-time alerts that are reviewed by our NOC/compliance staff, who may immediately suspend suspicious traffic pending investigation.

Quarantine or block calls linked to traceback requests or credible notices from regulators, law enforcement, or upstream carriers.

Maintain records of all alerts, investigations, and actions for audit and compliance purposes.

4) Remediation & Blocking Procedures

Business Information Solutions Inc. takes immediate action to block unlawful robocall traffic upon credible notice from the FCC, the Industry Traceback Group (ITG), upstream carriers, or our own analytics.

Immediate Suspension: When suspicious or flagged traffic is identified, we suspend the specific customer, telephone number, or route until investigation is complete.

Customer Notification & Remediation: We promptly notify the customer, provide details of the flagged traffic, and require them to submit evidence of remediation (such as proof of consent or updated campaign practices).

Termination of Repeat Offenders: Customers who fail to remediate or who are implicated in repeated incidents are permanently terminated from our network.

Recordkeeping: All remediation actions are logged, with details of the incident, customer response, and final resolution retained for audit and compliance purposes.

These procedures ensure that illegal traffic is immediately removed from our network, protect downstream carriers, and demonstrate our commitment to FCC robocall mitigation requirements.

5) Traceback Cooperation

Business Information Solutions Inc. fully cooperates with traceback requests from the FCC, the Industry Traceback Group (ITG), upstream carriers, and law enforcement. We commit to:

Responding to traceback requests within 24 hours of receipt.

Providing call detail records (CDRs), SIP signaling logs, and STIR/SHAKEN authentication information as needed to identify the source of traffic.

Maintaining call records for a minimum of 12 months to ensure traceability.

Taking immediate remedial action, including suspension or blocking of implicated traffic, when traceback confirms unlawful robocalls.

Our designated Traceback Point of Contact is: Phillip Long, CEO Email: plong@askbis.com Phone: 251-747-2959

6) Downstream/Reseller Controls

Business Information Solutions Inc. applies the same vetting and compliance requirements to resellers as to our direct customers. All resellers must:

Undergo KYC verification, including corporate registration, responsible party identification, and proof of right-to-use assigned numbers.

Agree contractually to implement STIR/SHAKEN where technically feasible and to enforce robocall mitigation practices across their own customers.

Flow down these obligations to any of their downstream clients.

Cooperate fully with traceback requests and FCC enforcement actions.

We continuously monitor reseller-originated traffic for compliance with expected baselines. If a reseller or one of their customers is delisted from the FCC Robocall Mitigation Database, or if credible notice is received of unlawful traffic, we will immediately block their traffic until remediation or termination.

7) Governance, Training, & Review

Business Information Solutions Inc. maintains executive-level accountability for its robocall mitigation program.

Responsible Executive: Phillip Long, CEO, is designated as the executive responsible for oversight of robocall mitigation compliance.

Employee Training: All relevant staff, including provisioning, network operations, customer onboarding, and support teams, receive annual training on FCC robocall mitigation requirements, STIR/SHAKEN policies, Know-Your-Customer procedures, traffic monitoring, traceback response, and remediation protocols. Training completion is documented and tracked.

Periodic Review: This Robocall Mitigation Plan is reviewed quarterly by the compliance team and immediately updated following any FCC rule change or enforcement action that impacts our obligations. Internal audits are performed to verify adherence to KYC, monitoring, and remediation processes.

Escalation: Compliance issues or repeat customer violations are escalated to the Responsible Executive, who determines final actions including service termination when warranted.

Through executive accountability, documented staff training, and regular plan reviews, Business Information Solutions Inc. ensures its robocall mitigation program remains effective, current, and aligned with FCC requirements.

Certification

Business Information Solutions Inc. hereby certifies compliance with 47 C.F.R. § 64.6300 et seq., including the implementation of STIR/SHAKEN caller ID authentication protocols on all IP-based portions of our network where technically feasible, and the adoption of a detailed Robocall Mitigation Plan for any portions not covered by STIR/SHAKEN.

We further certify that:

Our mitigation plan is filed and maintained in the FCC's Robocall Mitigation Database.

We will update this filing as required by FCC rule changes or material changes to our mitigation practices.

We will fully cooperate with traceback requests, respond within 24 hours, and maintain executive-level accountability for our robocall mitigation program.