

CLICK IT CONNECT CORP

Robocall Mitigation Program Description

(47 CFR § 64.6305)

1. Overview and Applicability

Click IT Connect Corp (“Company”) operates voice services utilizing IP-based and interconnected VoIP infrastructure, including SIP trunking, hosted PBX, and interconnection with upstream carriers and downstream customers. This Robocall Mitigation Program (“Program”) applies to all call origination, transit, and termination traffic handled by the Company and is designed to comply with 47 CFR § 64.6305 and related FCC guidance.

2. Network Architecture and Traffic Flow Controls

The Company’s network includes:

- SIP-based switching and routing platforms.
- Session Border Controllers (SBCs) for signaling and media control.
- Interconnection with upstream carriers and downstream enterprise and reseller customers.
- Traffic monitoring and call detail record (CDR) analysis systems.

Traffic is subject to policy-based routing, rate limiting, anomaly detection, and access control at network ingress and egress points.

3. Customer Onboarding and Risk Assessment (KYC/KYB)

The Company implements Know Your Customer (KYC) and Know Your Business (KYB) procedures prior to service activation, including:

- Verification of legal entity identity, ownership, and business purpose.
- Review of anticipated calling use cases, volumes, and geographic targets.
- Assessment of risk indicators such as automated dialing, outbound campaign use, and high-volume calling patterns.

- Contractual prohibitions against illegal robocalling, caller ID spoofing, and violations of the TCPA, TSR, and FCC rules.

Customers deemed high risk are subject to enhanced review and ongoing monitoring.

4. Upstream Provider Due Diligence

The Company conducts due diligence on upstream providers, including:

- Verification of regulatory compliance and interconnection legitimacy.
- Review of STIR/SHAKEN capabilities and attestation practices.
- Confirmation, where applicable, of listing in the FCC Robocall Mitigation Database.
- Periodic review of inbound traffic patterns from upstream providers.

5. STIR/SHAKEN Implementation

The Company has implemented STIR/SHAKEN authentication and verification across applicable IP network segments. Attestation levels (A, B, C) are assigned based on customer identity verification and call origination context. Where STIR/SHAKEN is not available due to technical or interconnection limitations, the Company applies this Program as a compensating control.

6. Traffic Monitoring and Analytics

The Company employs automated and manual monitoring of call traffic using CDR analysis and signaling inspection, including detection of:

- Abnormal call origination rates (calls per second/minute/hour).
- Short-duration calls and high answer-seizure ratio anomalies.
- Invalid or suspicious caller ID patterns.
- Traffic consistent with known robocall, scam, or fraud signatures.
- Geographic or destination-based anomalies.

7. Mitigation and Enforcement Actions

Upon identification of suspicious or illegal robocall activity, the Company may:

- Throttle or block call traffic at the SBC or switch level.
- Suspend or terminate customer SIP credentials or service accounts.
- Notify upstream providers or downstream customers.
- Preserve logs and CDRs for investigative purposes.
- Report activity to regulatory authorities or industry traceback organizations.

8. Traceback Cooperation

The Company commits to full cooperation with traceback requests from the FCC, law enforcement agencies, and the industry traceback consortium, including responding within 24 hours where required. The Company maintains technical and administrative processes to identify call sources and provide supporting records.

9. Logging, Record Retention, and Audit

The Company maintains logs and CDRs sufficient to support traceback and compliance obligations, including:

- SIP signaling logs and SBC event logs.
- Call detail records and routing metadata.
- Customer account and provisioning records.

Records are retained in accordance with internal policy and applicable regulatory requirements.

10. Continuous Improvement and Governance

The Company reviews this Program periodically to address evolving robocall threats, network changes, and regulatory developments. Updates are implemented as necessary and reflected in the FCC Robocall Mitigation Database when material changes occur.

11. Regulatory History Disclosure

Click IT Connect Corp discloses whether it or any affiliate has been subject to FCC, FTC, or law enforcement actions related to illegal robocalls within the past two years.