

Robocall Mitigation Program Description

Current Technology Solutions, LLC d/b/a Current TEK Solutions

Legal Entity	Current Technology Solutions, LLC
DBA	Current TEK Solutions
Business Address	5627 State Route 15, Bryan, Ohio 43506
Filing Type	Voice Service Provider Filing
Foreign Voice Service Provider	No
STIR/SHAKEN Certification	Option 3: No STIR/SHAKEN Implementation
Voice Service Provider Role	Voice Service Provider without a STIR/SHAKEN implementation obligation
Robocall Mitigation Contact	Marc Thomas, Founder & CEO / Executive Management
Contact Email	compliance@currentteksolutions.com
Contact Telephone	(419) 636-6200

1. Purpose and Scope

This Robocall Mitigation Program Description describes the reasonable steps Current Technology Solutions, LLC d/b/a Current TEK Solutions (the "Company") takes to avoid originating illegal robocall traffic and to cooperate with traceback requests. This description is submitted in support of the Company's Robocall Mitigation Database filing as a Voice Service Provider without a STIR/SHAKEN implementation obligation.

The Company provides hosted VoIP services to end-user business customers. The Company does not operate as a gateway provider or non-gateway intermediate provider based on its current service model. The Company does not provide wholesale call transit for other voice service providers. The Company serves business customers that use the Company's hosted voice services for ordinary business communications.

2. STIR/SHAKEN Implementation Status and Applicable Rule

The Company has selected Option 3: No STIR/SHAKEN Implementation. The Company has not implemented the STIR/SHAKEN authentication framework on any portion of its own network.

The Company is unable to implement STIR/SHAKEN directly because it lacks control over the network infrastructure necessary to implement STIR/SHAKEN. The Company provides hosted VoIP service through an upstream hosted voice platform/provider. The Company does not own or operate the underlying switching infrastructure, SIP network infrastructure, SPC token, STI certificate, or STIR/SHAKEN signing and attestation platform used for PSTN connectivity.

The Company does not make STIR/SHAKEN attestation decisions and does not sign calls using its own STI certificate. Network-level call authentication, PSTN interconnection, routing, carrier controls, and related technical controls are controlled by the Company's upstream hosted voice platform/provider. The Company maintains its own robocall mitigation program for the customer-facing portions of its hosted VoIP operations and cooperates with the upstream provider and authorities when suspicious or illegal calling activity is identified.

3. Customer Due Diligence and Know-Your-Customer Procedures

The Company provides hosted VoIP services primarily to known business customers. Before providing service, the Company takes reasonable steps to understand the customer, the nature of the customer's business, and the expected use of the service. The Company's customer due diligence may include reviewing customer identity, business name, service address, contact information, billing information, authorized users, and the customer's expected voice service use.

The Company does not knowingly provide service to customers that intend to originate illegal robocalls, unlawful spoofing, fraudulent calling campaigns, or other prohibited traffic. The Company may request additional information when a customer's use case, order size, traffic pattern, billing information, service address, or requested calling capability appears unusual or inconsistent with ordinary business communications.

The Company maintains customer account records, service records, numbers assigned to customers, service addresses, billing contacts, and support history. Customer service and technical support personnel may escalate unusual or suspicious activity to management for review.

4. Acceptable Use, Customer Restrictions, and Enforcement

The Company prohibits use of its hosted VoIP services for illegal robocalls, unlawful spoofing, fraud, scam calling, abusive calling, harassment, or any calling activity that violates applicable law, regulation, carrier policy, upstream provider policy, or the Company's service terms.

If the Company identifies or receives notice of suspected illegal robocall activity, unlawful spoofing, fraud, or materially suspicious calling activity associated with a customer account, the Company may investigate the activity, contact the customer, restrict outbound calling, suspend service, remove numbers, terminate service, or coordinate with its upstream hosted voice platform/provider to block or stop the traffic.

The Company will not knowingly assist any customer in evading call blocking, traceback, caller ID authentication, carrier restrictions, or regulatory requirements.

5. Monitoring, Analytics, and Traffic Review

The Company does not directly operate its own network-level robocall analytics platform and does not directly contract with a separate third-party robocall analytics vendor for this purpose. The Company relies on its upstream hosted voice platform/provider for network-level traffic controls, call authentication infrastructure, carrier-level fraud controls, traceback support, and any traffic analytics or blocking controls provided through the underlying hosted voice platform.

The Company also reviews operational indicators available to it, including customer reports, support tickets, billing anomalies, call detail records when available, usage spikes, unusual outbound call volume, repeated failed calls, unusual destination patterns, account changes, and notifications from upstream providers, carriers, law enforcement, the Commission, or the industry traceback consortium.

When suspicious traffic is identified, the Company may work with the customer and the upstream hosted voice platform/provider to review the activity, determine whether the traffic is legitimate, and take reasonable action to stop suspected illegal or abusive traffic.

6. Upstream Provider Due Diligence

The Company uses reputable upstream hosted voice platform/provider relationships to deliver PSTN-enabled hosted VoIP service. The Company maintains information regarding the upstream provider(s) used to deliver hosted voice service and will update those records when upstream provider relationships materially change.

The Company expects upstream provider(s) to maintain applicable FCC compliance programs, robocall mitigation controls, caller ID authentication infrastructure where applicable, fraud controls, and traceback cooperation procedures. The Company will cooperate with upstream provider(s) to investigate suspicious traffic, respond to traceback requests, and stop illegal robocall traffic that may use the Company's service to originate calls.

7. Traceback Response Commitment

The Company commits to respond fully within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use the Company's service to originate calls.

The Company's robocall mitigation contact is Marc Thomas, Founder & CEO / Executive Management, who can be reached at compliance@currentteksolutions.com and (419) 636-6200. The Company will review traceback requests promptly, identify relevant customer and call records available to it, coordinate with its upstream hosted voice platform/provider as needed, and take reasonable steps to stop any confirmed or suspected illegal robocall traffic.

8. Investigation and Remediation Process

Upon receiving a credible complaint, traceback request, upstream provider notice, law enforcement inquiry, Commission inquiry, or internal alert regarding suspected illegal robocall traffic, the Company will take reasonable steps to investigate. Those steps may include reviewing the customer account, call records available to the Company, assigned telephone numbers, service history, billing information, support notes, technical configuration, and upstream provider information.

If the Company determines that a customer is using the service to originate illegal robocalls or other prohibited traffic, or if the Company cannot reasonably validate the legitimacy of the traffic, the Company may restrict, suspend, or terminate the customer's ability to place outbound calls and may coordinate with the upstream hosted voice platform/provider to block the traffic. The Company may also preserve relevant records and cooperate with the Commission, law enforcement, and the industry traceback consortium.

9. Recordkeeping and Program Maintenance

The Company will maintain records reasonably necessary to support its robocall mitigation program, including customer account information, service records, assigned numbers, support tickets, traceback request records, escalation notes, and communications with upstream provider(s) related to suspected illegal robocall traffic.

The Company will review and update this program as needed based on changes to the Company's service model, upstream provider relationships, regulatory requirements, or known robocall mitigation risks. The Company will update its Robocall Mitigation Database filing within the time required by applicable FCC rules when required filing information changes.

10. Prior Formal Actions or Investigations

To the Company's knowledge, the Company has not, at any time in the prior two years, been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the Company transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or due to a deficient Robocall Mitigation Database certification or mitigation program description.

11. Officer Certification Support Statement

The Company submits this Robocall Mitigation Program Description to support its Robocall Mitigation Database certification. The Company understands that the officer signing the filing certifies under penalty of perjury that the filing is true and correct. The Company will maintain this program and will cooperate with regulators, law enforcement, the industry traceback consortium, upstream provider(s), and affected parties to investigate and stop illegal robocall traffic associated with the Company's service.

Prepared for Robocall Mitigation Database filing. Date: May 28, 2026.