

ROBOCALL MITIGATION PLAN

Techwebhosting Internet Solutions, LLC

FRN 0031327521 | PO Box 64, Shelbyville, KY 40066

Filed pursuant to 47 C.F.R. § 64.6305 | September 2026

1. Provider and Role

Techwebhosting Internet Solutions, LLC ("Techwebhosting") is a voice service provider offering hosted business telephone (cloud PBX) service to business customers located in Kentucky, delivered on a NetSapiens hosted platform operated by Techwebhosting. Outbound calls are terminated through licensed upstream carriers, including Flowroute. Techwebhosting originates calls only for its own contracted end-user customers. It is not an intermediate, gateway, or wholesale provider and does not accept or route traffic from any other voice service provider. Techwebhosting is not a foreign voice service provider.

Robocall mitigation contact

David Anderson, Co-Owner | abuse@techwebhosting.com | (502) 890-2042

Principals

David Anderson, Co-Owner | support@techwebhosting.com | (502) 890-2042

Aaron Henry, Co-Owner | support@techwebhosting.com | (502) 890-2042

DBAs: EdgeNode

Affiliates, subsidiaries, parent companies, other FRNs, prior names: None

2. STIR/SHAKEN Status

Techwebhosting has not yet implemented STIR/SHAKEN using a certificate issued to Techwebhosting, because it does not yet hold an SPC token; obtaining the token requires a Form 499-A filing, an OCN, and this RMD listing, which Techwebhosting is completing in the required order. Until then, all outbound calls are delivered to STIR/SHAKEN-participating upstream carriers that attest to and sign them. Techwebhosting will update this filing within ten business days of beginning to sign calls with its own certificate.

3. Know-Your-Customer

Techwebhosting does not offer anonymous or self-service signup for voice service. Voice service is provisioned only through a direct sales and onboarding process, and before outbound calling is enabled for any customer, Techwebhosting:

- verifies the customer is a real, operating business (business name, physical service address, state registration, and the identity of the authorizing owner or officer);
- reviews the intended use of the service, including expected call volumes and any need for international calling, and declines customers whose intended use is inconsistent with ordinary business telephone service;
- executes a written service agreement with an Acceptable Use Policy prohibiting illegal robocalls, caller ID spoofing, and telemarketing in violation of the TCPA or the Do Not Call rules, and permitting immediate suspension for suspected violations; and
- assigns only telephone numbers allocated to Techwebhosting or ported in with the customer's Letter of Authorization, and installs and provisions the customer's devices itself.

4. Technical Controls

- Each user and device has an individual, randomly generated SIP credential; no shared or default passwords; credentials are rotated on any indication of compromise.
- International dialing is disabled by default and enabled only on written request for specific countries after review; premium-rate and high-fraud-risk destinations are blocked platform-wide.
- Every customer domain and user has concurrent-call limits sized to actual seat count, and outbound rate limits per user and per domain, so a compromised endpoint cannot generate dialer-style volumes.
- Outbound caller ID is constrained by the platform to numbers assigned to the customer's domain.
- Outbound routing permits only Techwebhosting customer domains to egress through Techwebhosting carrier trunks; dial plans and route tables are audited on a schedule and after every change.

5. Monitoring, Detection, and Response

Techwebhosting enables platform fraud and velocity alerts that notify staff in real time when a user or domain exceeds call-attempt, concurrent-call, or international-call thresholds, and staff review call detail records each business day for anomalies including volume spikes, large numbers of unique destinations, short uniform durations with high answer rates, calls to invalid numbering ranges, off-hours calling, and unauthorized international attempts. Carrier fraud notices and traceback requests are treated as priority incidents.

On any indication of illegal or unauthorized calling, Techwebhosting immediately suspends outbound calling for the affected user or domain, revokes and reissues credentials where compromise is suspected, investigates using CDR, registration, and provisioning logs, notifies upstream carriers, and restores service only after the root cause is closed. Customers who knowingly originate illegal traffic are terminated.

6. Traceback and Cooperation

Techwebhosting commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the Industry Traceback Group, and retains CDRs and access logs for at least 18 months for that purpose. Requests should be directed to the contact in Section 1. Techwebhosting sends traffic only to upstream carriers listed in the Robocall Mitigation Database and verifies that listing before routing to any new carrier.

7. Enforcement History and Certification

Neither Techwebhosting nor any principal or affiliate has been the subject of any Commission, state, or law-enforcement action or investigation concerning illegal robocalls or caller ID spoofing. No prior certification of Techwebhosting has been removed from the Robocall Mitigation Database, and Techwebhosting is not barred from filing. All calls originated on the Techwebhosting network are subject to the practices described in this plan. Techwebhosting reviews this plan at least annually, updates its RMD filing within ten business days of any change, and recertifies by March 1 each year.

Certifying officer: David Anderson, Co-Owner **Date:** September 15, 2026