



Computers@WORK dba Modern Telephone Company

ROBOCALL MITIGATION PLAN UPDATED – FEBRUARY 2026

1. PURPOSE AND SCOPE

Computers@Work (the "Provider") is a voice service provider that originates voice traffic to the public switched telephone network (PSTN) and maintains a robocall mitigation program consistent with 47 CFR § 64.6305, including STIR/SHAKEN caller ID authentication implemented pursuant to 47 CFR § 64.6301(a).

2. PROVIDER ROLE / CALL FLOW

The Provider operates as a cloud PBX provider serving local small businesses, typically of 5–25 extensions each. End users place outbound calls only through phones and extensions provisioned and controlled by the Provider. The Provider manages provisioning and service configuration on its platform. The Provider physically installs and administers customer phone systems and supports ongoing operations for established customer relationships. Calls route from customer endpoints through the Provider's platform to Bandwidth for PSTN interconnection.

3. STIR/SHAKEN STATUS

The Provider certifies that it has implemented Complete STIR/SHAKEN caller ID authentication for calls it originates on its IP network, consistent with 47 CFR § 64.6301(a). The Provider's network is entirely IP-based, and the Provider fully signs all calls that originate on its network.

Signing / authentication approach: The Provider uses third-party providers to support its STIR/SHAKEN implementation. Telonium serves as the Certificate Authority and issued the Provider's signing certificate. Bandwidth performs hosted signing for the Provider's originating traffic; calls are signed prior to handoff for downstream verification by terminating providers.

4. ROBOCALL MITIGATION MEASURES

a. KNOW YOUR CUSTOMER / ONBOARDING CONTROLS

The Provider limits customer calling capabilities to devices and extensions provisioned on the Provider's managed phone system and does not permit customers to originate traffic outside of that controlled environment. The Provider primarily serves customers with long-standing business relationships and performs in-person installation and configuration of phone systems at the customer's premises, or via authenticated deployment workflows where in-person is not feasible. During onboarding, the Provider collects and verifies business identity information (e.g., legal business name, address, responsible party, and service location details) and validates that the customer is a legitimate operating business before enabling outbound calling. If onboarding



information is inconsistent, unverifiable, or suggests elevated risk, the Provider delays activation pending enhanced review and/or declines service.

b. **TRAFFIC MONITORING, ANALYTICS, AND ENFORCEMENT**

Monitoring Controls: All outbound calling activity is controlled and observable within the Provider's platform. The Provider uses custom scripts that review call logs every 15 minutes to detect anomalies and indicators of attempted illegal access or misuse, including (as applicable) unusual calling bursts, abnormal short-duration patterns, suspicious destination profiles, and unexpected changes in calling behavior. In addition, the Provider's carrier, Bandwidth, monitors outbound voice traffic in real time using network-level analytics and call authentication/verification signals to identify and help prevent the origination of suspected illegal robocall traffic, and the Provider coordinates with Bandwidth on any escalations, restrictions, or remediation actions as needed.

Investigation & Response: When an anomaly is detected, the Provider investigates promptly by reviewing call detail records and account activity, validating the source extension/device, and confirming legitimacy with the customer when needed. The Provider may apply immediate mitigations including temporary call restrictions, outbound blocking, credential resets, forced re-authentication, suspension of impacted extensions, or full service suspension pending resolution.

Enforcement: The Provider enforces acceptable use requirements through customer notice, corrective action requirements, suspension/termination for repeated or egregious violations, and cooperation with upstream providers and enforcement entities where appropriate.

c. **CALLER ID INTEGRITY AND ANTI-SPOOFING CONTROLS**

Caller ID Authorization: The Provider provisions caller ID numbers to customers and restricts presentation to numbers assigned and/or validated for that customer account.

Configuration Controls: Administrative access to routing, trunking, and caller ID settings is restricted to authorized personnel using least-privilege access.

5. TRACEBACK COOPERATION AND RESPONSE

The Provider remains committed to responding fully and within 24 hours to call traceback requests from the Commission, law enforcement, and the traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers initiating calls.

6. PROGRAM GOVERNANCE AND PLAN MAINTENANCE

The Provider reviews and maintains its robocall mitigation program and updates it as needed when services, traffic patterns, or risk controls change. The Provider will update its RMD filing and associated plan information within 10 business days when filing information changes.