

WebFones, LLC

Robocall Mitigation Plan

Updated: May 8, 2026

1. Purpose and Provider Information

This Robocall Mitigation Plan is submitted by WebFones, LLC, headquartered at 505 Beachland Blvd., Suite 262, Vero Beach, FL 32963.

WebFones provides voice services and may act in one or more roles in the call chain, including as a voice service provider serving end-user customers, a wholesale originating provider, and a non-gateway intermediate provider. WebFones has implemented robocall mitigation practices designed to prevent the origination, transmission, and processing of illegal robocalls through its network.

WebFones has not been prohibited from filing a certification in the FCC Robocall Mitigation Database. WebFones does not have a history of enforcement actions for illegal robocalls, TCPA violations, TSR violations, or related state-law violations.

2. Provider Roles in the Call Chain

WebFones may perform the following roles in the call chain:

- Voice service provider with a STIR/SHAKEN implementation obligation serving end-user customers;
- Voice service provider with a STIR/SHAKEN obligation acting as a wholesale provider originating calls;
- Non-gateway intermediate provider with a STIR/SHAKEN obligation.

WebFones applies robocall mitigation procedures to outbound voice traffic regardless of WebFones' role in the call chain for a particular call.

3. Know Your Customer / Customer Vetting Procedures

WebFones conducts Know Your Customer ("KYC") and customer vetting procedures for new and existing customers before allowing customers to originate voice traffic through the WebFones network.

As part of this process, WebFones collects and reviews customer-identifying information, which may include the customer's legal business name, physical address, billing information, responsible contact, business purpose, website or other public business presence, intended calling use case, and telephone numbers to be used as caller ID. WebFones uses this information to confirm that it has an authenticated relationship with the customer and to evaluate whether the customer's use of voice services appears legitimate.

WebFones also reviews whether the customer or its principals are known to be subject to enforcement actions, restrictions, or other information indicating that the customer may be prohibited from initiating certain types of calling, including illegal robocalls, spoofing, unlawful telemarketing, TCPA violations, TSR violations, or similar conduct.

Where applicable, WebFones validates that the customer has a legitimate right to use the telephone numbers it asserts as caller ID. This may include numbers assigned by WebFones, numbers ported to WebFones, numbers assigned by another provider, or numbers otherwise authorized for the customer's use. WebFones uses this information to support the caller ID authentication attestation level assigned to calls originated for that customer.

WebFones' contractual provisions and acceptable use policies prohibit customers from using WebFones services to originate illegal robocalls, unlawful spoofed calls, fraudulent calls, or other unlawful traffic. If WebFones identifies suspicious or potentially unlawful traffic associated with a customer, WebFones may investigate the traffic, require additional information from the customer, restrict calling, block traffic, suspend service, terminate service, or take other appropriate action.

If WebFones determines that a customer is originating traffic that is likely unlawful or presents a material robocall risk, WebFones may suspend or terminate the customer's service without prior notice where necessary to prevent further unlawful traffic.

4. Caller ID Authorization and Attestation Practices

WebFones follows caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers.

WebFones reviews customer-identifying information to confirm that it has an authenticated relationship with the customer. WebFones also evaluates whether the customer has a legitimate right to use asserted calling numbers, including numbers assigned by WebFones, numbers ported to WebFones, numbers assigned by another provider, or numbers otherwise authorized for the customer's use.

WebFones uses customer vetting and caller ID authorization information to support the attestation level assigned to calls originated for the customer. WebFones does not knowingly allow customers to use caller ID numbers that they are not authorized to use.

WebFones may review invalid numbers, unallocated numbers, unassigned numbers, Do-Not-Originate numbers, caller ID reputation information, traceback information, and other available data to determine whether a call or calling pattern presents a robocall mitigation concern.

5. Upstream Provider Review

WebFones maintains a vetting and review process for upstream providers that send voice traffic to WebFones for termination, transit, or other processing.

Before accepting traffic from an upstream provider, WebFones reviews the provider's identity, role in the call path, Robocall Mitigation Database filing status, and robocall mitigation practices. WebFones will not knowingly accept voice traffic directly from a provider that is required to be listed in the Robocall Mitigation Database but does not have an active RMD filing.

WebFones seeks to understand the upstream provider's role in the call path, including whether the provider is acting as an originating voice service provider, wholesale provider, foreign intermediate provider, U.S.-based intermediate provider, gateway provider, or other provider type. WebFones uses this information to evaluate call authentication obligations and robocall mitigation risk.

WebFones requires upstream providers to maintain reasonable robocall mitigation practices, comply with applicable FCC rules, cooperate with traceback requests, and refrain from sending unlawful robocall traffic to WebFones.

If WebFones identifies suspicious or potentially unlawful traffic from an upstream provider, WebFones may investigate the traffic, request additional information, require corrective action, restrict traffic, block traffic, suspend traffic acceptance, terminate the provider relationship, or take other appropriate action.

6. Robocall Mitigation Program

WebFones uses call analytics software and network monitoring tools, including tools provided by TransNexus, to monitor outbound voice traffic and identify potentially suspicious or unlawful calling activity.

These tools may identify traffic involving invalid, unallocated, unassigned, or Do-Not-Originate numbers; poor caller ID reputation; unusual calling patterns; high-volume calling inconsistent with the customer's expected use case; short-duration call patterns; repeated call attempts; traceback-related concerns; or other indicators of potentially unlawful robocall activity.

WebFones reviews alerts and other suspicious traffic indicators to determine whether a customer, upstream provider, or other traffic source may be attempting to originate, transmit, or facilitate unlawful robocalls. WebFones applies mitigation procedures to outbound traffic regardless of WebFones' role in the call chain for a particular call.

If WebFones identifies suspicious traffic, WebFones may investigate the source of the traffic, review customer or upstream provider information, request additional information, require corrective action, restrict traffic, block traffic, suspend service, terminate service, or take other appropriate action.

WebFones maintains the right to take immediate action where necessary to prevent unlawful robocalls, fraudulent traffic, spoofed calls, or other traffic that presents a material risk to consumers, the telephone network, or WebFones' compliance obligations.

7. Traceback Cooperation

WebFones responds within the required timeframe to traceback requests from the FCC, law enforcement, and the registered traceback consortium.

WebFones maintains procedures to receive, log, investigate, and respond to traceback requests. When responding to a traceback request, WebFones reviews available call detail records and related account information to identify, when available, the customer, upstream provider, downstream provider, call date and time, calling number, called number, call routing information, and any other information reasonably necessary to assist with the traceback.

WebFones cooperates with the FCC, law enforcement, the registered traceback consortium, and other appropriate entities in investigating and stopping illegal robocalls that originate, transit, or are otherwise processed through WebFones' services.

If a traceback or related investigation indicates that a customer or upstream provider is using WebFones services to originate or transmit unlawful robocalls, WebFones may require corrective action, restrict traffic, block traffic, suspend service, terminate service, or take other appropriate action.

8. STIR/SHAKEN Implementation

WebFones has implemented STIR/SHAKEN for calls it originates where technically feasible and required by FCC rules. WebFones has its own STIR/SHAKEN certificate issued through the TransNexus Certification Authority and uses a STIR/SHAKEN solution supplied by TransNexus to authenticate calls that WebFones originates.

WebFones applies caller ID authentication based on its relationship with the customer, the customer's right to use the calling number, and WebFones' ability to identify the customer and the calling party. WebFones uses customer vetting and caller ID validation information to support the attestation level assigned to originated calls.

For traffic received from other providers, WebFones evaluates the role of the upstream provider and the authentication status of the traffic in accordance with applicable FCC rules and industry standards. Where WebFones receives unauthenticated or improperly authenticated traffic that presents a robocall mitigation concern, WebFones may investigate, restrict, block, or refuse such traffic as appropriate.

9. Suspension, Blocking, and Termination Procedures

WebFones' customer agreements, contractual provisions, acceptable use policies, and provider relationships prohibit the use of WebFones services to originate, transmit, or facilitate illegal robocalls, fraudulent traffic, spoofed calls, unlawful telemarketing, or other unlawful traffic.

When WebFones identifies suspicious or potentially unlawful traffic, WebFones may take one or more mitigation steps depending on the nature, severity, and urgency of the issue. These steps may include investigation, customer or provider outreach, requests for additional information, warnings, traffic restrictions, call blocking, suspension of service, termination of service, refusal to accept traffic, or other appropriate action.

WebFones may take immediate action, including suspension, blocking, or termination, where necessary to prevent ongoing unlawful traffic, protect consumers, respond to traceback or law enforcement concerns, comply with FCC requirements, or protect the integrity of the telephone network.

10. Recordkeeping and Ongoing Review

WebFones maintains records related to customer identity verification, caller ID authorization, upstream provider review, traffic monitoring, robocall mitigation investigations, traceback responses, corrective actions, suspensions, and terminations where applicable.

WebFones periodically reviews its robocall mitigation practices, customer vetting procedures, upstream provider relationships, traffic analytics, and RMD filing information to confirm that its procedures remain accurate and reasonably designed to prevent unlawful robocall traffic.

WebFones may update this Robocall Mitigation Plan as necessary to reflect changes in WebFones' operations, provider roles, tools, procedures, FCC rules, industry standards, or other relevant compliance obligations.

11. Robocall Mitigation Database and CORES Update Commitment

WebFones will review its Robocall Mitigation Database ("RMD") filing on an ongoing basis and will update its RMD filing within 10 business days of any change to information required to be submitted in the RMD.

This includes, but is not limited to, changes to WebFones' provider role, ownership or control, business identity, contact information, traceback contact information, STIR/SHAKEN implementation status, robocall mitigation practices, uploaded robocall mitigation plan, or any other information required by FCC rules.

WebFones will also update its FCC CORES/FRN registration information within 10 business days of any change to information submitted in CORES.

WebFones will maintain internal procedures to periodically review the accuracy of its RMD and CORES information and to ensure that required updates are submitted within the applicable FCC deadline.