

Robocall Mitigation Plan – Westelcom Networks, Inc.

Robocall Mitigation Compliance with TRACED Act

Date	On behalf of	Change Summary
November 22, 2024	Westelcom Networks, Inc. – OCN 1227	Revised 11/22/2024

Objective: Establish and follow a policy that is compliant with TRACED Act

Westelcom Networks, Inc. (WESTELCOM) is a small competitive local exchange carrier with headquarters at 3330 State Highway 11B, Nicholville, NY 12965.

WESTELCOM performs the following role in the call chain:

- A voice service provider with a STIR/SHAKEN implementation servicing end users
- A voice service provider with a STIR/SHAKEN obligation acting as a wholesale provider originating calls
- A non-gateway intermediate provider with a STIR/SHAKEN obligation

WESTELCOM is a wholly owned subsidiary of SDC Atlas Acquisitionco LLC. WESTELCOM is managed by SLIC Network Solutions, Inc.

WESTELCOM has not been prohibited from filing a certification in the Robocall Mitigation Database.

WESTELCOM does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations.

WESTELCOM uses the affirmative, effective measures described herein to prevent to origination or transit of illegal robocalls. All WESTELCOM traffic is subject to such mitigation.

I. Implementation and Extension Status

Extensions Received Under 47 C.F.R. §64.6304

WESTELCOM is eligible for the continuing extension of the STIR SHAKEN implementation deadline as a small voice service provider (§64.6304 (a)(2) that has non-IP portions within its network §64.6304(d).

WESTELCOM, through its ownership, is a member of NTCA who participates on the ATIS Non-IP taskforce working group which developed the (ATIS Solutions) non-IP call authentication solutions and serves as WESTELCOM's third-party representative on the ATIS Non-IP taskforce working group.

Robocall Mitigation Plan – Westelcom Networks, Inc.

Status of STIR/SHAKEN Implementation

WESTELCOM has registered with the STI-PA using OCN 1227. WESTELCOM has our own STIR/SHAKEN certificate issued by TransNexus STI-CA. WESTELCOM has implemented STIR/SHAKEN using an STI-AS and STI-VS supplied by TransNexus.

The portion of WESTELCOM traffic that remains TDM is subject to its robocall mitigation plans.

II. General Prohibition Against Illegal Robocalling

WESTELCOM end user services are subject to restrictions pursuant to its Acceptable Use Policies and Terms of Service (“TOS”) requirements. WESTELCOM Acceptable Use Policies and TOS published on its website will be updated to reflect the illegality of robocalling including the prohibition against:

- Providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call
- Violating any applicable local, state, or federal law; using WESTELCOM service to engage in or in connection with fraudulent activities such as illegal robocalling.

In addition, WESTELCOM is updating its TOS to expressly reference the prohibition on robocalling and all current subscribers will receive notice of the publication of its updated TOS.

III. Robocalling Mitigation

Analytics

WESTELCOM utilizes ClearIP call analytics software by TransNexus, a third-party analytics vendor, to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls.

The software provides detailed reporting to identify suspected illegal robocalls. The system alerts us if WESTELCOM processes outbound calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list.

WESTELCOM performs the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call.

WESTELCOM immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If WESTELCOM determines that the traffic was likely unlawful, then WESTELCOM will warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then WESTELCOM will terminate their service.

Robocall Mitigation Plan – Westelcom Networks, Inc.

IV. Know Your Customer

WESTELCOM follows the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group.

WESTELCOM has a "know your-customer policy" to assist in preventing its voice services from being used to originate illegal robocall traffic. WESTELCOM identifies potential business customers prior to providing service by collecting information such as their physical business location, contact person(s), federal tax ID, and the general nature of their business. In addition:

- A WESTELCOM representative may visit the premise of a business to verify the number of users at the location is appropriate for the volume of outbound calls.
- WESTELCOM will not deploy large volume calling capability as a residential service or at an address shown in the company records as being residential.

WESTELCOM serves a small number of long-time business customers with large volume calling capability that have been directly contacted to review with them WESTELCOM's policies and efforts to prevent WESTELCOM's network from being used for illegal robocalling.

V. Know Your Upstream Provider

WESTELCOM has a vetting and review process for upstream providers, that is, providers that send us voice traffic that WESTELCOM terminates or transits to other providers.

WESTELCOM confirms that the upstream provider has a certification in the Robocall Mitigation Database. WESTELCOM will not accept voice traffic from an unregistered provider.

WESTELCOM requires that the upstream provider has a reasonable robocall mitigation plan, including a vetting process for its customers and upstream providers, and uses call analytics to identify suspicious traffic.

WESTELCOM establishes an understanding of the upstream provider's role in the call path for the traffic they will send to us, for example, whether they are acting as an originating voice service provider, a foreign intermediate provider, or a U.S.-based intermediate provider. We use this information to understand whether we will be obligated to authenticate unsigned traffic that we receive from them.

WESTELCOM contractual provisions with upstream providers prohibit them from sending us illegal robocalls. If WESTELCOM finds that an upstream provider is sending us suspicious robocalls, WESTELCOM will warn them to stop. If such traffic continues, then WESTELCOM will terminate their service.

Robocall Mitigation Plan – Westelcom Networks, Inc.

VI. Traceback and Enforcement Cooperation

WESTELCOM will actively participate with the traceback community including the FCC, law enforcement, and The Industry Traceback Group (ITG). WESTELCOM commits to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the ITG and will cooperate with such entities in investigating and stopping any illegal robocallers that use our services to originate calls.