

Robocall Mitigation Plan Cherokee Cablevision

This robocall mitigation plan is for Cherokee Cablevision, with headquarters at 28 John Crowe Hill Drive, Cherokee, NC 28719. Cherokee Cablevision resells interconnected VoIP services provided by BalsamWest FiberNet, LLC to retail end-users in Western North Carolina. Cherokee Cablevision does not own or operate switching, numbering, or STIR/SHAKEN authentication infrastructure. All underlying voice network functions are provided by BalsamWest FiberNet, LLC.

We perform the following role in the call chain:

- A retail voice service provider (VoIP reseller) furnishing access to voice service to end-users with our internet services and interconnectivity to BalsamWest FiberNet.

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

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

Know Your Customer

Cherokee Cablevision follows caller ID authentication best practices for vetting customer identity and operational legitimacy consistent with FCC guidance and industry standards and have validated with our underlying provider that they adhere to the same standards.

- We collect and review entity-identifying information sufficient to confirm a legitimate customer relationship.
- We prohibit customers from initiating unlawful robocalls in our service agreements.
- We do not knowingly permit the origination of illegal robocalls.

Cherokee Cablevision relies on BalsamWest FiberNet, LLC, as the underlying facilities-based voice provider, to perform network-level call authentication, analytics monitoring, and mitigation functions.

Traceback

Cherokee Cablevision cooperates fully with the Commission, law enforcement, and the registered traceback consortium.

Because all voice traffic is provisioned and transported over BalsamWest FiberNet's voice network, traceback requests involving Cherokee Cablevision customers are coordinated immediately with BalsamWest FiberNet to ensure investigation and response within 24 hours.

Robocall Mitigation Program

Cherokee Cablevision relies on the robocall mitigation program implemented by BalsamWest FiberNet, LLC, which includes:

- Real-time outbound traffic monitoring and analytics.
- Investigation of suspicious or unlawful traffic.
- Enforcement actions including customer warnings and service termination when appropriate.

Cherokee Cablevision maintains contractual provisions that prohibit customers from initiating illegal robocalls. If suspicious traffic is identified, Cherokee Cablevision coordinates with BalsamWest FiberNet to investigate and take appropriate corrective action.

Cherokee Cablevision does not have direct access to numbering resources, SIP signaling control, or STIR/SHAKEN authentication infrastructure.

STIR/SHAKEN

Cherokee Cablevision does not operate its own STIR/SHAKEN authentication infrastructure.

All STIR/SHAKEN implementation obligations associated with the voice traffic furnished to Cherokee Cablevision customers are fulfilled by BalsamWest FiberNet, LLC, as the underlying interconnected VoIP provider and network operator.

Cherokee Cablevision relies on BalsamWest FiberNet's STIR/SHAKEN compliance and certificate management for authentication of calls originated by Cherokee Cablevision retail customers. Below is BalsamWest's published Mitigation plan.

Robocall Mitigation Plan for BalsamWest FiberNet, LLC

This robocall mitigation plan is for BalsamWest FiberNet, LLC, with headquarters at 35 Bonnie Lane, Sylva, NC 28779. BalsamWest is a small CLEC in Western North Carolina currently offering only landline VoIP services.

We perform the following roles in the call chain:

- *A voice service provider with a STIR/SHAKEN implementation obligation serving end-users*

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

BalsamWest FiberNet does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations. BalsamWest FiberNet uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls.

Know Your Customer

We follow 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. This process includes the collection and review of entity-identifying information to confirm that we have an authenticated relationship with the customer. We use this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls. We also validate, when possible, that the entity has a legitimate right to use its asserted calling numbers. We use this information to support the attestation level we assign to calls that we originate for that customer.

Our contractual provisions with customers prohibit them from initiating illegal robocalls. If we find a customer initiating suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

Traceback

We respond within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. We cooperate fully with such entities in investigating and stopping any illegal robocallers that use our service to originate, carry, or process illegal robocalls.

Robocall Mitigation Program

We use call analytics software provided by TransNexus 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 we process outbound calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list. We immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.

STIR/SHAKEN

We have registered with the STI-PA using OCN 801D. We have our own STIR/SHAKEN certificate issued by the TransNexus Certification Authority (STI-CA) that we use when authenticating calls we originate.

We have implemented a STIR/SHAKEN solution supplied by TransNexus.

We are exempt from STIR/SHAKEN implementation requirements for some calls because these calls rely on non-IP technology - 47 CFR 64.6304(d).