

Robocall Mitigation Plan 2/11/2026

This Robocall Mitigation Plan is formally submitted for MIX Networks, Inc., with headquarters at 608 Robin Rd., Lakeland, FL 33803.

MIX Networks, Inc. performs the following role in the call chain:

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

MIX Networks, Inc. has not been prohibited from filing a certification in the Robocall Mitigation Database.

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

MIX Networks, Inc. uses the following measures to prevent the origination or transit of illegal robocalls.

MIX Networks KYC (Know Your Customer) Policies

MIX Networks adheres to best practices for caller ID authentication for vetting caller identity and operational legitimacy for our new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group.

This process includes collection and detailed review of identifying information to confirm that we have an authenticated relationship with the end customer. We use the information we collect to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do or if they are prohibited from initiating telemarketing/robocall-type calls.

Our platform and terms of use forbid the “spoofing” of phone numbers. We also validate, when possible, that customers have a legitimate right to use its asserted calling numbers. We use this information to support the attestation levels that we assign to calls.

Our network does not support any high-volume robocall-type traffic, as this is restricted not only by our own policies and terms of use, but also by the policies and networks of our underlying service providers.

Additionally, our contractual provisions with end user customers prohibit them from sending any high volume, fraudulent, abusive, or illegal robocall-type traffic. If we find that a customer is initiating suspicious calls, we block/suspend their services and advise them that services will remain suspended while we investigate their suspicious calling activity. If the calling activity is found to be in violation of our policies, we warn them to immediately cease sending such traffic. If such traffic continues despite the warning, we then disconnect and terminate their services.

MIX Networks Know Your Upstream Provider Policies

We have a vetting and review process for upstream providers (providers/vendors who may send us voice traffic that we terminate or transit to other service providers).

We first confirm that the upstream provider has an entry and certification in the Robocall Mitigation Database. We do not accept voice traffic from any unregistered service providers.

We require that upstream providers have a robocall mitigation plan which must include a vetting process for their customers and upstream providers. They also must use call analytics to identify suspicious traffic.

Our contractual provisions with upstream providers prohibit them from sending us illegal robocalls. If we find that an upstream provider is sending us suspicious robocalls, we warn them to stop. If such traffic continues despite the warning, we would terminate services.

Traceback

MIX Networks responds 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 illegal robocallers who attempt to use our service to originate, carry, or process illegal robocalls.

Robocall Mitigation Program

MIX Networks uses 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 perform the same robocall mitigation steps for all outbound calls regardless of our role in the call chain for a particular call.

We promptly investigate any 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

MIX Networks has registered with the STI-PA using OCN 856H/FRN0014166573. 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 full STIR/SHAKEN solution (through TransNexus) under RMD14166573 and are actively signing calls with the appropriate attestation levels, A, B, or C.

Thank You –

MIX Networks, Inc.