

UsVox, Inc. Robocall Mitigation Program Description

Overview:

UsVox, Inc. Complete full STIR/SHAKEN Implementation. This includes continuous call origination monitoring, stringent upstream provider vetting and advanced call authentication protocols. 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 perform the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call.

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. These measures are designed to identify and block suspicious call attempts while maintaining full compliance with FCC regulations.

We have registered with the STI-PA using OCN 823K. 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 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.

We have a vetting and review process for upstream providers, that is, providers that send us voice traffic that we terminate or transit to other providers.

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

We require that upstream providers have a reasonable robocall mitigation plan, including a vetting process for their customers and upstream providers, and 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, 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.

Key Elements of the Program:

Call Origination Monitoring:

- Continuous monitoring of call volume patterns to detect anomalies indicative of potential robocall activity using advanced tools provided by TransNexus Clear IP.
- Use of automated systems to identify and flag suspicious calling patterns, including:
 - High-volume calls from single numbers.
 - Unusual calling times.
 - Geographically inconsistent calling behavior.

STIR/SHAKEN Implementation:

- Full adoption of the STIR/SHAKEN framework through TransNexus ClearIP to authenticate call origination.
- Rejection of calls with invalid or missing call attestation information.
- Regular monitoring and updates to ensure optimal performance of STIR/SHAKEN call authentication.

Real-time Call Analysis:

- Deployment of advanced call analytics tools through TransNexus ClearIP to identify and block calls exhibiting characteristics commonly associated with robocalls, including:
 - Spoofed numbers.
 - High-risk caller IDs.
 - Suspicious calling patterns.

Complaint Handling Process:

- Operation of a dedicated complaint handling system to efficiently receive and investigate customer reports of suspected robocalls.

- Prompt response to complaints, including:
 - Thorough analysis of call data.
 - Implementation of appropriate actions to address the source of the robocall activity.

Network Security Measures:

- Implementation of robust network security protocols to prevent unauthorized access and potential misuse of UsVox network for generating robocalls.
- Regular vulnerability assessments and updates to maintain a secure network environment.

Compliance and Reporting:

- Full adherence to all applicable FCC regulations related to robocall mitigation.
- Regular reporting on robocall mitigation activities, including:
 - Analysis of call volumes.
 - Complaint trends.
 - Actions taken to address potential robocall issues.

Contact Information:

For reporting suspected robocalls or inquiries related to our robocall mitigation program, please contact UsVox support team at:

Email: support@usvox.com

Phone: 786-275-5888 option # 3

Website: www.usvox.com

UsVox, Inc. remains committed to protecting our customers and maintaining the integrity of our network through proactive and effective robocall mitigation strategies.