

Robocall Mitigation Plan

This robocall mitigation plan is for Convergent Software, d.b.a. Convergent Communications, with headquarters at 900 County Road 950, Calhoun, TN 37309

We perform the following roles in the call chain:

- A voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- Our downstream carrier is Bandwidth.com

Convergent Software, d.b.a. Convergent Communications has not been prohibited from filing a certification in the Robocall Mitigation Database.

Convergent Software, d.b.a. Convergent Communications does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations.

Convergent Software, d.b.a. Convergent Communications 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.

In addition, we have implemented a Call Abuse Policy, as it pertains to the TRACED Act, and have published the following policy to our terms of use:

*“Any call originated on the **Convergent Communications** network is subject to inspection and investigation if the call is suspected of being fraudulent, abusive, or illegal. Calls meeting any of these criteria will be blocked. If these conditions are repeated, becoming excessive, the subscriber may be disconnected from **Convergent Communications**’ network, may be subject to further investigation by the FCC for enforcement of the TRACED Act and the subscriber may be subject to fines and penalties imposed by the FCC or the jurisdictional court.”*

Know Your Upstream Provider

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

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.

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.

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 have also developed in-house automatic call analytic monitoring that alerts us when various robocall indicators are triggered.

- We verify that the answered calls to unanswered calls ratio exceeds a threshold to validate that the call recipient expected to speak with the calling entity as determined by caller ID.

- We verify that the call duration of answered calls exceeds a threshold that would validate that the call recipient is intentionally engaged with the calling entity.
- We verify that a percentage of calls to the corresponding area code of the calling number exceeds a threshold that would validate that the calling entity is primarily contacting established customers which would tend to be in the same area code.
- We are alerted when the number of outbound calls per hour exceeds a threshold not likely to be met by our clients.

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 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 967k. 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.