

Robocall Mitigation Program Description

Zray Technologies Corporation, 12585 Kirkham Ct., Poway, CA 92064. Roseville, CA 95678.

Preventative Measures

We perform the following roles in the call chain:

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

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

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

Zray Technologies uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls.

Caller Identification

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, including: checking robocalls, unallocated calls and invalid numbers against a pre-existing "Do Not Originate" list; use of reputation scoring (i.e., caller ID analysis/lookup) to determine whether a call likely was executed with malicious intent; block lists; and dynamic traffic analysis.

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 and acceptable user policy 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 have the right to terminate or suspend their service, reserving all rights and remedies including injunctive (restraining) relief.

Upstream Providers

We have a vetting and review process for upstream providers, those are 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.

We establish 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.

Our contractual provisions and acceptable use policy with upstream providers endeavors to 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 the allotted time 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 perform mitigation steps for all outbound calls regardless of our role in the call chain for a particular call.

We promptly 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 suspend or terminate their service.

STIR/SHAKEN

We have our own STIR/SHAKEN certificate issued by the TransNexus Certification Authority (STI-CA) that we use when authenticating calls that we originate. We have implemented a STIR/SHAKEN solution supplied by our equipment vendors.