

Robocall Mitigation Plan

This robocall mitigation plan is for VIP2PHONE INC, with headquarters at 8400 NW 36th St Suite 450,Doral, FL 33166.

We perform the following roles in the call chain:

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

VIP2PHONE INC has not been prohibited from filing a certification in the Robocall Mitigation Database.

VIP2PHONE INC does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations.

VIP2PHONE INC 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.

All new subscribers go through an onboarding process that includes data gathering stages and verification. VIP2PHONE INC does not activate clients that provide anonymous information, or where data mismatches are found.

Robocall Mitigation Plan for VIP2PHONE INC

All subscriber outbound calls against a third party service, which provides in return a risk score. Calls above a certain threshold get blocked automatically. There are also automated filters in place that identify abusive behavior (calling of the same number multiple times, calling of multiple numbers in a short period of time from the same callerid, etc).

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 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 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.

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 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.

STIR/SHAKEN

We have registered with the STI Policy Administrator (STI-PA) using OCN 799J.

VIP2PHONE INC maintains valid STIR/SHAKEN certificates issued by authorized STI Certification Authorities.

We have implemented a STIR/SHAKEN solution supplied by TransNexus, including certificate management, call analytics, and Out-of-Band SHAKEN capabilities for calls that rely on non-IP technology.

In addition, VIP2PHONE INC uses its internally managed Kamailio platform to authenticate and sign outbound calls using STIR/SHAKEN certificates issued by Telonium, an authorized STI Certification Authority.

This hybrid architecture enables VIP2PHONE INC to apply appropriate attestation levels based on customer vetting and caller identity verification, while maintaining redundancy, control, and compliance with FCC and ATIS STIR/SHAKEN requirements.