

Zella Technologies LLC

Robocall Mitigation Plan

This robocall mitigation plan is for Zella Technologies LLC, with headquarters at 43233 S Airport Rd, STE 101, Hammond, LA 70403.

We perform the following roles in the call chain:

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

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

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

Zella Technologies LLC 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.

Know Your Upstream Provider

We maintain formal procedures to identify, vet, and continuously monitor all upstream voice service providers from whom we accept traffic. These procedures are designed to ensure call quality, regulatory compliance, and the prevention of illegal robocall traffic entering our network.

Prior to accepting traffic from any upstream provider, we perform a due diligence review that may include verification of the provider's legal identity, regulatory status, Robocall Mitigation Database certification, STIR/SHAKEN implementation posture, and network reputation. We assess the provider's

history of traffic quality, complaint rates, and ability to cooperate with traceback and enforcement requests.

We require upstream providers to comply with applicable federal and state laws governing robocalls, caller ID authentication, and voice traffic delivery. Upstream providers are expected to cooperate fully with traceback investigations and to take prompt corrective action if unlawful traffic is identified.

We continuously monitor upstream traffic for indicators of illegal or abusive calling behavior, including abnormal calling patterns, elevated complaint rates, invalid or spoofed caller ID usage, and high-risk traffic characteristics. If suspicious activity is detected, we promptly investigate and may implement mitigation actions including enhanced monitoring, traffic blocking, rate limiting, or suspension of traffic. Continued transmission of unlawful traffic may result in termination of the provider relationship.

Traceback

We respond within 24 hours to all traceback requests from the Commission, law enforcement, and the ITG. 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 Sansay and in-house software 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 that may trigger as suspicious.

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 traffic is likely unlawful, we issue warning notices and require immediate corrective action. Mitigation actions may include warning notices, traffic blocking, rate limiting, suspension, or termination, depending on the severity and persistence of the activity. 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 647K. We have our own STIR/SHAKEN certificate issued by the Sansay Certification Authority (STI-CA) that we use when authenticating calls we originate. We have implemented a STIR/SHAKEN solution supplied by Sansay.