

Servpac Incorporated
Robocall Mitigation Plan

Updated: February 2024

Introduction

This document details the steps taken by Servpac Incorporated (“Servpac” or “Company”) to mitigate illegal robocalling.

Servpac provides voice services to non-residential subscribers. The voice communications services that we provide include both Voice over IP (VoIP) technology as well as TDM services. For the latter services, Servpac resells the underlying services of Hawaiian Telecom and does not own or control facilities that would enable it to implement the STIR/SHAKEN authentication framework on those calls and relies on Hawaiian Telecom’s underlying capabilities for that functionality. Hawaiian Telecom’s RMD registration identifies it as Partial STIR/SHAKEN implementation due to its non-IP network. Accordingly, Servpac is also registering as Partial implementation to reflect the portion of its voice calling that utilizes resold TDM services.

For its interconnected voice services that are provided entirely over IP networks, Servpac is an STI-GA authorized Service Provider registered with the Secure Telephone Identify Policy Administrator (STI-PA) and participates in the Signature-based Handling of Asserted Information Using toKENs (SHAKEN) ecosystem. It relies on Bandwidth, its underlying carrier, as well as services and software provided TransNexus to authenticate its originating calls and for other robocall mitigation practices, as described herein.

Know Your Customer

Servpac follows 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 vet upstream providers that send us voice traffic that we terminate to confirm that the provider has a certification in the Robocall Mitigation Database and a reasonable robocall mitigation plan, including a vetting process for their customers and upstream providers. We also use call analytics provided by TransNexus 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.

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. Our contact email for traceback requests is:

legal@servpac.com

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