

MULTITEL LLC
4103 Oak Tree Cir
Rochester, MI, 48306
legal@multitel.net

Contact Information:

Dan Caescu
CEO
586-204-0040
dan.caescu@multitel.net
OCN: 610J
Updated: 2024/02/19

Robocall Mitigation Plan

This robocall mitigation plan is for MULTITEL LLC, with headquarters at 4103 Oak Tree Cir, Rochester, MI, 48306.

We perform the following roles in the call chain:

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

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

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

MULTITEL 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. MultiTEL does not activate clients that provide anonymous information, or where data mismatches are found.

As part of this onboarding process, customers go through a KYC process where biometric data is collected using a 3rd party identity verification service (withpersona.com), which gathers biometric data and official documents such as IDs, passports, driver's licenses , etc .

A risk score is developed to ensure the authenticity of a new subscriber. This score checks the identity markers collected during an account registration process. These include but are not limited to: name, e-mail address, physical address, credit card information, contact phone number, signup IP address.

These identity markers are validated for accuracy against public and paid tools. Furthermore, we check that signup IPs are not VPNs (against known IP ranges used by various VPN providers), and that the signup IPs geo data matches the area code of the contact phone number and, where this information is available, that the credit card issuer information also matches the geolocation provided by IP address and NPA/NXX of the phone number.

All new subscribers receive by default a capacity of only two simultaneous outbound calls. This ensures that, in the event where a new subscriber decides to place robocalls through our network, their total volume of calls would be very low, as a two simultaneous call limit would not scale for high volume operations, but rather to manually dialed numbers only.

All subscriber activity is further monitored as explained below:

- periodic checks are done to ensure that the channels are not used 100% of the time. In case a 100% usage of channels is seen for extended periods of time, further manual checks are done (calling the source numbers to find out if IVRs indicative of telemarketing activities are answering the calls, checking the source numbers against various online sources for the purposes of finding complaints – if any, checking SIP logs for known robocalling agents (such as vicidial, for example), and so on)
- checking every outbound calls against a third party service (TransNexus's ClearIP 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-PA using OCN 610J. 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.