



Company Summary

Micronesian Telecomm. Corp. dba IT&E is a ILEC in CNMI. With commercial offerings, IT&E enables service providers and businesses to transact and communicate with their customers. -

Robocall Mitigation Plan

Micronesian Telecomm. Corp. uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls.

Know your Customer

Micronesian Telecomm. Corp. dba IT&E takes reasonable steps to avoid originating or carrying illegal Robocalls within its network. CFR 64.1200(n)(4) This includes steps to know its customers.

Micronesian Telecomm. Corp. follows the best practice for vetting its customers' caller id using the best practice for implementation of Call Authentication outline in NANC Call Authentication Trusted Anchor Working Group. Ref. <https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf> As part of the process of getting to know our customers, Micronesian Telecomm. Corp. collects and reviews customer information, which is also reviewed to determine if the customer is subject to any enforcement action or has taken part in any illegal call activity.

Our contractual provision with our customers prohibits them from initiating illegal robocalls. If determined that a customer is initiating suspicious robocalls, we will notify customers to cease sending the suspicious traffic. If the customer continues to originate suspicious calls after receiving notification IT&E has the right to terminate their service.

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 providers have a certificate in the Robocall Mitigation Database..



We will not accept any traffic from any Voice Service Provider, Non-Gateway Intermediate Provider who is not registered or listed in the RMD database.

We require that upstream providers have a reasonable robocall mitigation plan, including 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 us. This information is used to determine whether we are 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 sends us calls that are suspicious and determined to be illegal robocalls, we alert them of the calls and inform them to cease sending such calls. If the upstream provider continues to send us suspicious/illegal robocall traffic, we have the right to 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, and process illegal robocalls.

STIR/SHAKEN

We have registered with the STI-PA using OCN 3700. We have our own STIR/SHAKEN certificate issued by the TransNexus Certification Authority (STI-CA). Authentication and verification of voice traffic we use TransNexus ClearIP STIR/SHAKEN solution.

Call Analytics

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 reserve the right to terminate their service.