

AllCloudIP LLC

Robocall Mitigation Plan

SUMMARY/BACKGROUND

The FCC has adopted rules requiring voice service providers to implement Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) caller identification authentication technology in the Internet protocol portion of their networks. In addition, the FCC is requiring all providers to implement a Robocall Mitigation Plan to ensure that providers are actively stopping illegal calling on their networks.

AllCloudIP LLC is a reseller of Voice over Internet Protocol (VoIP) systems. The following are the Robocall

Mitigation steps we have taken to comply with the FCC mandate.

VOICE CUSTOMER VERIFICATION

AllCloudIP LLC does a due diligence audit of each of our customers. Since we install a switch, router, and phones at each customers location we are required to know the nature of the customer business in detail. Our due diligence audit will:

1. Verify the physical address of the customer.
2. Verify the contact person who is a decision maker on telephony issues.
3. Verify the customers voice needs and thoroughly understand the nature of the customers business.

All our customers are required to have a static IP address with their Internet Service Provider that we use to program their router. We own the router and only allow voice traffic to traverse the router.

STIR/SHAKEN

We have complied with the FCC STIR/SHAKEN policies and our implementation is completed. AllCloudIP LLC has worked with their SIP Trunk Provider to ensure that the outbound calls are compliant with STIR/SHAKEN.

ROBOCALL MITAGATION IMPLEMENTATION

All customers who use AllCloudIP LLC as a VoIP service provider are subject to the following policies regarding phone calls originating on the Trunks and DID's that are used

on any system or device. These procedures and requirements are also in place to prevent unauthorized access to our systems, which also prevents robocalling problems.

Every customer has a static IP that they use to access voice services. This IP address is used as an Access Control List (ACL) in multiple redundant firewalls. Only the ACLs in the firewall are allowed to access the system.

1. Each phone is password protected with a unique identity to discourage nefarious actors from accessing the phone remotely.
2. All traffic coming from our routers is monitored. Any traffic that seems to be higher than normal and/or has high volume, short duration traffic is scrutinized to ensure that no unlawful intrusions have taken place.
3. Call Detail Records are monitored to ensure that they are consistent with the company's history.
4. Server access logs are reviewed to make sure no unauthorized person or entity tried to access them remotely.
5. In real-time, we have the ability to monitor all incoming and outgoing calls from every PBX that we manage.
6. AllCloudIP has a policy of allowing an end user to only output a phone number for Caller ID that resides on our network and legally owned by the customer
7. We monitor CERT related messages to ensure that all our current security practices are meeting the current threats.

TRACEBACK

We respond to all traceback requests from the FCC, law enforcement and the registered traceback consortium and cooperate with such entities in investigating and stopping any robocalls that originate on our network. In addition, we implement best practices published by the Traceback Consortium.