

CSX Cloud Robocall Mitigation Plan

The FCC requires voice service providers to develop a Robocall Mitigation Plan that:

- Details the reasonable steps that are taken to avoid originating illegal robocalls
- Demonstrates a commitment to participate in traceback requests and to cooperate with investigations to stop illegal robocalls
- Is filed in the Robocall Mitigation Database to certify a full implementation of STIR/SHAKEN or the institution of a Robocall Mitigation Plan

So let's talk about the steps we're taking to mitigate robocalls and illegal spoofing.

Fraud Prevention

We are a Software As A Service provider where we manage the customer interactions using our hosted customer solutions software systems, this includes, email, fax, telecommunications, online interaction, video and web chat. We fully manage and control all interactions with restrictions in place to prevent the capability for robocalling. Our software does not allow nor support robocalling. Our users are unable to use any type of automated dialing or dialer outside of the software as a service that we provide in our subscription. Each user has a user name and complex password tied back to their unique PBX server, customers do not share instances. Each caller has a preset Caller ID and each company has a CNAM registration. Calls made from other sources or incorrect user and passwords are blocked and the IP is added to a blocked list. Our customers are carefully screened using Know Your Customer (KYC) and each user signs an acceptable use agreement with our software subscriptions. CSX Cloud acts to maintain valid registrations in the FCC's Robocall Mitigation Database ("RMD") and requires clear service-specific contractual requirements in which

customers agree to cooperate and agree to follow all applicable laws against illegal robocalling, fraud and abuse. After our initial “KYC” onboarding screening, CSX Cloud’s operations personnel stay closely aligned with its customers and the industry’s anti-robocalling efforts and developments to remind, educate and clarify what behaviors may signal or constitute unlawful robocalling, and continually notify customers when we identify instances that need their attention in order to prevent illegal robocalling behaviors using their software services.

Proactive Monitoring

We have a robust monitoring platform utilizing industry-leading technology that performs SIP analytics and call detail record (CDR) analysis in real-time. This allows us to identify potentially illegal robocalling on our network.

CSX Cloud has a team of operational experts who have implemented technical and operational processes and procedures to monitor, detect and analyze the use of its services and traffic on our network that helps to determine when illegal and inappropriate robocalling activity may be occurring. CSX Cloud has deployed a “Call Blocking Tool” that incorporates industry best practices into its core solutions to identify and block invalid, unallocated and otherwise obviously illegal telephone numbers. Further, even though it acts predominantly as an “Software As A Service Provider”, CSX Cloud implemented STIR/SHAKEN in its all-IP communications long before it was mandated by the FCC and has been working to increase call detail transparency and collaborative traceback enablement for years. When unlawful robocall campaigns are attempted, CSX Cloud follows established processes and procedures to notify upstream customers of the problematic traffic and request that they take immediate corrective actions to prevent reoccurrence of the illegal calls. CSX Cloud’s engagement and support also includes work to monitor that its customers to ensure they are effectively cooperating and working to address the sources of each traceback event. CSX Cloud consistently analyzes its call detail records to identify problematic call patterns and their sources from where it sits in a myriad of traffic flows. Bandwidth then incorporates these learnings into its traffic data analytics and

detection technologies to continually improve its capabilities to accurately detect suspected illegal activity and deploy mitigation measures.

Through this platform, we can detect large bursts of calls in a short timeframe through dynamic traffic analysis; identify patterns of low average call duration and/or low completion rates through CDR analytics; identify large numbers of calls from invalid numbers; review common caller ID name (CNAM) values across service providers; and detect calls from numbers that are invalid, unallocated, unassigned or listed on Do Not Originate (DNO) registries.

Extensive Investigation

Our real-time monitoring platform identifies suspicious calls or calling patterns, we will seek to identify the party that is using our network to originate, route or terminate these calls. Our investigation can include verifying that the originating customer owns (or is authorized to use) the caller ID number, suspending the offender's ability to originate or terminate calls on our network, and/or initiating a traceback investigation completed fully within 24 hours.

A traceback investigation is the process of determining the origin of a call, typically starting with the receiving party and terminating voice service provider and tracing backwards through the path to the origin of the call. CSX Cloud does take corrective action to terminate service arrangements with customers that put CSX Cloud at risk. CSX Cloud's commitment to the benefits of STIR/SHAKEN in an all-IP network environment advances improvements in accurate and targeted call blocking that are designed to block calls from invalid and illegal telephone numbers in keeping with industry best practices and the FCC's recommendations, while simultaneously work to prevent anti-competitive and discriminatory blocking and mislabeling that is unfortunately plaguing the competitive industry with overly broad and blunt analytics. CSX Cloud can work closely with Law Enforcement Agencies (LEA) at all levels of government and with its interconnected carrier partners. CSX Cloud's fraud and security experts are constantly working to respond to complaints and trouble tickets with customers that may be associated with the unlawful uses of CSX Cloud's services. In addition to these notifications, we then aim to work diligently together

with our customers and other industry members to stop the unlawful robocall campaigns being detected. Finally, together with its active involvement, CSX Cloud supports the industry's established Do Not Originate (DNO) efforts pursuant to the industry best practices and procedures.

Across all of its service provider roles CSX Cloud continues to have fraud mitigation success with its three-pronged operational approach (prevent, detect, and mitigate) that incorporate FCC mandates and industry best practices for each of its roles as described above.