

InnAcloud

Robocall Mitigation Plan

Know Your Customer

We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

Traceback

We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls.

STIR/SHAKEN Extensions

We are eligible for and are taking STIR/SHAKEN implementation extension received under 47 CFR § 64.6304 because we have fewer than 100,000 voice subscriber lines. All the voice traffic that originates on our network is subject to the robocall mitigation program described below.

Robocall Mitigation Program

Policy: InnAcloud Technologies, LLC has contractually committed to immediately stop using, and/or cause our customers and End Users to immediately stop using, the impacted Services if we suspect or have knowledge of any fraudulent use of the Services. Customer will contact InnAcloud immediately if Customer becomes aware at any time that Customer's Service is being stolen, fraudulently used or otherwise being used in an unauthorized manner. We are committed to working with our upstream provider, and if we become aware of unusual Service-related volumes or patterns, will make an effort to stop any fraudulent use of the Services. We reserve the right to block any actual, alleged or suspected fraudulent use of the Services without prior notice.

We use custom developed software to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls.

Combining behavioral analytics, caller authentication and verification, our solution features:

Fraud Detection: Detection of high volume robocalling, spoofing and spam call activity. INNACLOUD systems Monitor Normal Call patterns and detect Abnormalities in Call volume / destination / Source numbers and will Alert Customers and Persons at INNACLOUD. INNACLOUD networks monitor for suspicious call patterns and only accepts calls from its Known customers and known IP addresses. Suspicious call patterns include short duration calls to random numbers within a short period of time, many calls to incrementing destination numbers, within a short period of time. Other algorithms are also used to determine suspicious activity on INNACLOUD networks.

INNACLOUD Will Block all calls from unknown Source numbers. INNACLOUD uses only Source numbers that are assigned and ported to its Network. Customers Must Submit a List of all Source Numbers that are Outside of the INNACLOUD network and verify that they are authorized to use such source numbers.

Subscriber Notification: Caller ID Name override to warn subscribers of suspicious calls.

Call Blocking Support: Accurate identification enabling you to block fraudulent phone calls as per the TRACED Act (2019)

Business Number Verification: Register legitimate business numbers to prevent unintentional call blocking. INNACLOUD only offers services where it services the end user PBX system that produces the Source calls to its network. These PBX systems only allow Caller ID of specifically programmed source numbers. These PBX systems monitor for suspicious call patterns, such as high volumes of short-duration calls within short period of time.

Caller ID Name Service: Easy integration of Caller ID name lookup service, including robocall mitigation with override to include original caller ID even when call is determined fraudulent.