



iPlum

Robocall Mitigation Plan

iPlum Inc. has been in business since 2016. We are a technology company that helps businesses with a separate 2nd line on the mobile phone.

Robocall Mitigation – Overview

Customers are able to place calls originating from their iPlum registered phone number. Caller ID and call records are reviewed when service is installed to verify legitimate caller id Information. All iPlum originated calls traverse our server application stack, where they are sent upstream to our transit providers

We utilize call blocking technology to automatically block known robocall numbers and suspicious calls identified by analytics.

POLICIES

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>)

Know Your Customer (KYC) procedures

The new customers are required to provide a government issued ID verification when opening an account.

10-business-day material change update commitment

iPlum commits to maintaining the accuracy of its Robocall Mitigation Database filing. In accordance with 47 C.F.R. § 64.6305, iPlum will update its RMD certification and this mitigation plan within **10 business days** of any material change in its robocall mitigation practices, contact information, or STIR/SHAKEN implementation status."

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 have implemented STIR/SHAKEN in our network.

Robocall Mitigation Program

We use software provided by underlying carrier 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.

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.

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.

In addition, we have implemented a Call Abuse Policy and have published the following policy to our web site, terms of use, and have notified our customers of the policy as copied below:

“Any call originated on the Plum network is subject to inspection and investigation if the call is suspected of being fraudulent, abusive, or illegal. Calls meeting any of these criteria will be blocked. If these conditions are repeated, becoming excessive, the subscriber may be disconnected from the Plum network, may be subject to further investigation by the FCC for enforcement of the TRACED Act and the subscriber may be subject to fines and penalties imposed by the FCC or the jurisdictional court.”
