

AtlasV Robocall Mitigation Plan

Voice Service Provider Classification

AtlasV does not directly provide any network infrastructure associated with its applications but relies on our CLEC (Competitive Local Exchange Carrier) partners to act as the voice service providers. All voice traffic within AtlasV applications is initiated, transmitted, and terminated by our CLEC partners. Therefore, AtlasV itself is not obligated to implement the STIR/SHAKEN protocols but relies on its CLEC partners to authenticate voice traffic.

We are aware that our CLEC partners have completed the STIR/SHAKEN integration and have reported the relevant information in the Robocall Mitigation Database. Generally, calls initiated from AtlasV applications are signed by the CLEC using their own digital certificate and assigned a “B” attestation level.

Robocall Mitigation Plan

AtlasV applications are designed in a way that does not lend themselves to robocall implementations. We have not exposed any APIs or SDKs that could be leveraged for robocall solutions. All calls must be initiated by the application running on an iOS or Android device. Furthermore, account owners cannot hold more than one active call at a time.

We take proactive and effective measures to prevent new and returning customers from originating illegal calls. These measures include investigating all suspicious activities related to voice traffic on our applications.

We have implemented a call analytics system that monitors inbound/outbound call ratios and can identify suspicious calling patterns, including but not limited to sequential dialing and outgoing calls with high intensity within a specific time slot. User accounts exhibiting suspicious calling patterns are immediately flagged, and automatic action may be taken to deactivate the account, thereby preventing the user from making or receiving voice calls on the relevant application.

In addition to the anti-fraud measures performed by our U.S.-based CLEC partners, AtlasV proactively applies its own anti-fraud measures.

We will deactivate accounts if any fraudulent or abusive activities are reported. Once an account is deactivated, the user will no longer be able to make use of the services associated with that account.

We can blacklist callee numbers that have elected not to receive calls from phone numbers held by users of our products. We also provide mobile users with the ability to easily block calls from our mobile applications.

“Know-Your-Upstream Provider” Procedures

As stated above, AtlasV does not provide any network infrastructure associated with its applications but relies on CLEC partners to act as the voice service providers. Our CLEC partners

initiate, transmit, and terminate all voice traffic on our applications and deploy STIR/SHAKEN protocols to authenticate the traffic from our applications.

All inbound calls to our product users from any voice service provider will traverse through our CLEC partner's network and will be subject to the CLEC's robocall mitigation plan, as well as the measures undertaken by us.

Traceback Participation

AtlasV commits to fully and promptly participating in all legal requests for voice call tracebacks needed to combat robocalling, pursuant to the TRACED Act and other applicable laws and regulations.

AtlasV certifies that it has not been prohibited from filing in the Robocall Mitigation Database at any time. AtlasV also certifies that it is not subject to any FCC, law enforcement, or regulatory investigations related to robocalling.