



Robocall Mitigation Plan

The Laffoon Corporation dba Vertical Horizon Networks (VHN) provides Voice Over Internet Protocol (“VoIP”) services as a reseller of white-labeled services offered by IronSIP, LLC. (“IronSIP”). VHN does not control the softswitch, number porting or call trunking for the associated calls. Accordingly, VHN does not have the facilities necessary to implement STIR/SHAKEN. VHN’s origination provider IronSIP fully implements STIR/SHAKEN and attests ALL voice calls made from the VHN network. VHN has, however, adopted this robocall plan to establish procedures to limit the potential for originating, carrying, or processing unlawful robocalls through its voice services.

VHN certifies it has not been prohibited from filing in the Robocall Mitigation Database and VHN has not been subject to any Commission, law enforcement, or regulatory agency action or investigation arising from suspected unlawful robocalling or spoofing.

In accordance with 47 CFR § 64.6305(e), VHN has designated a point of contact to receive notice of illegal robocall traffic or other robocall mitigation-related issues. That person’s name, title, address, phone number and email are available in the Robocall Mitigation Database.

PROCEDURES TO MITIGATE OR STOP ROBOCALLS

I. Know Your Customer

VHN in partnership with IronSIP, follows the North American Numbering Council (“NANC”) Call Authentication Trust Anchor Working Group guidelines and best practices for vetting caller’s identity Best Practices for the Implementation of Call Authentication Frameworks. VHN confirms the identity of all of its customers including, but not limited to (i) contract person(s); (ii) business location, (iii) state or country of incorporation, (iv) federal tax identification; and (v) nature of our customer’s businesses throughout the customer’s service period.

II. Contractual Terms

Customers using VHN’s services agree to abide by the rules and regulations set forth in our “Acceptable Use Policy” and “Internet Terms and Conditions” Policies (Acceptable Use Policy and Terms of Use for Services Agreement). VHN’s Acceptable Use Policy and Terms of Use Agreement expressly prohibit customers/subscribers from engaging in illegal activity, creating a false Caller ID (i.e., spoofing) or robocalling.

Customers are informed that any suspicious activity will be investigated; and if the customer is engaging in, or has engaged in illegal robocalling, their service will be terminated.

III. Traceback Requests

VHN commits to respond fully to all traceback requests from the Commission, law enforcement, and the Registered Traceback Consortium within 24 hours. In the unlikely event illegal robocallers use VHN’s system to originate calls, VHN will cooperate with such entities’ investigation.



IV. Robocall Mitigation

VHN's underlying voice provider, IronSIP, has committed to fully complying with Commission's robocall blocking requirements and has confirmed that it will block all calls and provider traffic that: (1) are identified in any public notice or order released by the FCC; (2) are substantially similar to the types of traffic identified in any public notice or order released by the Commission; or (3) include a caller ID number or name that is on DNO list issued by ITF. IronSIP also blocks the traffic of all foreign providers and gateway providers that have not registered in the Robocall Mitigation Database.

V. Know Your Upstream Provider

VHN has an agreement in place with IronSIP to resell IronSIP's VoIP offering to VHN's customers. VHN has confirmed that IronSIP is listed in the Robocall Mitigation Database and IronSIP has "Know Your UpstreamProvider" provisions in place.

VI. Network Monitoring (Call Analytics Systems)

VHN's end-user services are subject to network monitoring that monitors against illegal robocalls such as high call volumes and high call duration. Designated employees review all flagged call patterns and actively resolve issues as quickly as possible. For whatever reason, if the end-user is uncooperative, VHN will implement mitigation activities not limited to suspension or termination of service.

IronSIP also has implemented a proprietary fraud detection and mitigation process that analyzes high volume network traffic to evaluate compliance. IronSIP utilizes a variety of fraud detection indicators and fraud prevention best practices. Calls from the VHN network are routed through to IronSIP to verify and certify calls. IronSIP also takes remedial action to prevent or remediate robocalling or other fraudulent activity it detects on its customers' systems.

If VHN's upstream provider IronSIP determines the call did not originate from VHN, the call will not be certified and will fail.

VII. Plan Updates

VHN will continue to monitor industry best practices and review internal processes to ensure our systems adapt to address the ongoing challenges affecting this industry.