

IP-Com, LLC (Robocall Mitigation Plan for FCC RMD Filing)

This Robocall Mitigation Plan has been prepared based on the latest Robocall Mitigation instructions on <https://www.federalregister.gov/documents/2023/06/21/2023-12142/call-authentication-trust-anchor>

It is being submitted on the Robocall Mitigation Database website and it will be updated as required, per instructions listed on the most recent notice <https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf>. Such as if any of the company's listed contact information (ex: address, Tel#, listed officer, etc.) changes.

(I). Status of STIR/SHAKEN Implementation

IP-Com, LLC fully implemented the STIR/SHAKEN authentication framework across its entire network using an FCC and iConectiv approved STIR SHAKEN vendor. IP-Com, LLC complies with 64.6301 Caller ID authentication requirements and other parts of FCC Robocall regulations. Such as those listed on <https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/subpart-HH> and does so by:

- (1) Authenticating and verifying caller identification information for all SIP calls that exclusively transit its own network;
- (2) Authenticating caller identification information for all SIP calls, it originates and that it will exchange with another voice service provider or intermediate provider and, to the extent technically feasible, transmits that call with authenticated caller identification information to the next voice service provider or intermediate provider in the call path; and
- (3) Verifying caller identification information for all SIP calls it receives from another voice service provider or intermediate provider, which it will terminate and for which the caller identification information has been authenticated.

(II). Robocall Mitigation Program

IP-Com, LLC uses software to monitor outbound voice traffic in real time to prevent the origination of illegal robocalls. The software provides detailed reporting to identify suspected illegal robocalls and alert IP-Com, LLC if it originates any calls where the calling number is invalid, unallocated. If IP-Com, LLC determines that the caller was attempting to originate unlawful robocalls, then IP-Com, LLC can either warn them to stop or terminate their service as appropriate.

(III). Know Your Customer

For each call, IP-Com, LLC determines the nature of the business of each of its customers, to ensure that they are not providing services to individuals or entities engaged in robocalling. Continuously monitoring traffic from them, to look for suspicious and unauthorized types of activity. Immediate action is taken in situations where it is deemed necessary to prevent illegal robocalling or other forms of prohibited behavior.

(IV). Traceback

IP-Com, LLC responds to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperates with such entities in investigating and stopping any illegal robocalls that attempt to use the systems of IP-Com, LLC.

(V). Robocall Mitigation Plan

The following is provided by IP-Com, LLC (hereafter “the Provider”) in compliance with RMD rules per <https://www.federalregister.gov/documents/2023/06/21/2023-12142/call-authentication-trust-anchor> and <https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf>. To describe the Provider’s updated robocall mitigation plan to the FCC RMD portal. This updated plan describes the specific “reasonable steps” that the Provider has taken to avoid, as applicable, the origination, carrying, or processing of illegal robocall traffic as part of its robocall mitigation program.

(1). Regarding the Commission’s updated regulations, “Requiring the First Intermediate Provider To Authenticate Unauthenticated Call”. Note that the Provider is a US-based carrier and on some calls, it plays the role of voice service provider serving US based end users making US to International calls or International to US calls. While on other calls, the Provider plays a role of gateway intermediate provider, which it understands has been defined by the FCC as the party that is the point of entry for foreign calls into the U.S. Where the Provider receives calls directly from a foreign originating carrier or foreign intermediate provider that the Provider transmits downstream to another US-based provider.

Where the Provider is the voice provider / party originating calls from US callers, it properly ensures the proper caller ID information when it passes the call to the next carrier in the chain. The Provider also ensures that it properly signs calls = its STIR/SHAKEN token for attestation is in the SIP header of the call before it passes the call to the next carrier in the chain. If the Provider is an intermediate provider / not the originating carrier, it will authenticate unauthenticated caller ID information. Specifically, it will require the FCC mandated Caller ID data has been included when it receives the call. Also, it will ensure that the carrier passing the call has properly attested the call with STIR/SHAKEN token in the SIP header before the Provider will pass the call to the next carrier in the chain. The Provider will fully respond within 24 hours to all traceback requests received from the Commission, law enforcement, and the industry traceback consortium.

Where the Provider is an Intermediate provider in the call and it has directly contracted with an originating provider, such contracts signed by the Provider will include language to require originating providers to properly include FCC mandated Caller ID data and their STIR/SHAKEN token attestation in the SIP header of the call. The contract language will require originating carriers to provide the Provider (as an intermediate provider) with data needed to perform Due diligence necessary to understand the sources of the traffic being sent by the Originating carrier. Where this focus on the beginning of the call path is meant at directly addressing the problem of calls entering the call path without authentication by originating providers. With the goal of stopping illegally spoofed robocalls and ensuring that the Provider as the first intermediate provider in the chain will know when it is receiving calls directly from the originating carrier vs. when the Provider is not the first intermediary in the call chain.

(2). Applicable STIR SHAKEN Standards For Compliance

The Provider will comply with the version of the STIR/SHAKEN standards ATIS–1000074, ATIS–1000080, and ATIS–1000084 and all of the documents referenced therein in effect at the time of their respective compliance deadlines, including any errata as of those dates or earlier. Where those standards can currently be downloaded from The Alliance for Telecommunications Industry Solutions (ATIS) website on <https://www.techstreet.com/atis/>. The Provider understands its responsibility to upgrade and maintain its network to stay in compliance with FCC standards, such as those outlined in § 64.6303 as listed on <https://www.govinfo.gov/content/pkg/CFR-2022-title47-vol3/pdf/CFR-2022-title47-vol3-sec64-6303.pdf>. To do so, the Provider has internal technical staff and outside vendors (ex: Certificate Authority/STA-CA vendor) review the STIR SHAKEN technical standards. The Provider will continue to review any FCC mandates regarding ATIS and any other STIR-SHAKEN standards that are to be implemented.

(3). Mitigation and Robocall Mitigation Database Filing Obligations

The Provider recognizes that the Commission requires downstream providers to block traffic received directly from all intermediate providers that are not in the Robocall Mitigation Database. The Provider will comply, and block traffic received directly from all intermediate providers that are not in the Robocall Mitigation Database (RMD) https://fccprod.servicenowservices.com/rmd?id=rmd_listings. The Provider's systems will check the Robocall Mitigation Database to see if intermediate providers trying to send traffic via the Provider are on the Robocall Mitigation Database. Before those intermediate providers are allowed to use the Provider's systems to pass on calls. This is in addition to the other requirements listed on the prior page, in terms of contract language and due diligence cooperation that will be required from intermediate providers that wish to work with the Provider.

(4). Applying the "Reasonable Steps" Mitigation Standard to All Providers

The provider will promptly investigate and mitigate illegal robocall traffic brought to the provider's attention through measures such as internal monitoring and tracebacks. As part of the reasonable steps that the Provider is taking to significantly reduce" the carrying or processing (for intermediate providers) or origination (for voice service providers) of illegal robocalls. The Provider understands that it must comply with the practices that its program requires, and that its program is insufficient if the Provider "knowingly or through negligence" carries or processes calls (for intermediate providers) or originates (for voice service providers) unlawful robocall campaigns. The Providers commits to respond fully, within the time period required by the Commission's rules, to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers that use its service to originate, carry, or process illegal robocalls.

(5). Expanded Robocall Mitigation Database Filing Obligations

The Provider recognizes that all providers' robocall mitigation plans must describe the specific "reasonable steps" the provider has taken to avoid, as applicable, the origination, carrying, or processing of illegal robocall traffic as part of its robocall mitigation program. Also, the requirement that if a provider plays more than one "role" in the call chain, that it should explain the mitigation steps it undertakes in each role, to the extent those mitigation steps are different. The Provider does play more than one "role" in the call chain as described on page 1. Since the Provider may be the originating provider on some calls, while it is the intermediate carrier on other calls. The Provider will take the reasonable robocall mitigation steps (ex: required call ID and STIR SHAKEN token attestation). As described on page 2, which will vary depending on whether it is the originate carrier, or intermediate provider in the call chain.

The Provider recognizes that Gateway providers are required to provide a description of how they have complied with the know-your-upstream provider requirement in § 64.1200(n)(4) of the Commission's rules. It will comply with the know-your-upstream provider requirement in § 64.1200(n)(4) of the Commission's rules. The Provider recognizes that Gateway providers must provide a description of how they have complied with the know-your-upstream provider requirement in section 64.1200(n)(4) of the Commission's rules. Where those rules require taking "affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic". The Provider will require the FCC mandated Call ID data has been included when it receives the call and that the carrier passing the call to the Provider has signed = proper STIR/SHAKEN token for attestation in the SIP header from the carrier passing the call to the Provider. Before the Provider passes that call to the next carrier in the chain and the Provider will fully respond within 24 hours to all traceback requests received from the Commission, law enforcement, and the industry traceback consortium. If the Provider has directly contracted with an originating provider, such contracts signed by the Provider will include language to require originating providers to properly include FCC mandated Caller ID data. In the event that the carrier (whether originating provider or intermediate provider) handing the call to the Provider is not able to obtain STIR SHAKEN tokens for attestation, such as if that carrier is a foreign entity, the Provider will take additional due diligence steps. Such as determining the business reputation of that carrier (ex: number of years incorporated/formed/in business, credit history, reputation within the industry, call analytics on calls sent by that carrier). In addition, the Provider will include language in the contract that will require originating carriers to provide the Provider (as an intermediate provider) to perform due diligence necessary to understand the sources of the traffic being sent by the carrier.

For all calls, the Provider will comply with Section 64.1200(n)(5) of the Commission's rules. To "take reasonable and effective steps to ensure that any originating provider or intermediate provider, foreign or domestic, from which it directly receives traffic is not using the provider to carry or process a high volume of illegal traffic onto the U.S. network. The Provider recognizes that gateway providers for particular calls must, with respect to those calls, "block any calls purporting to originate from a number on a reasonable do-not-originate list. A list so limited in scope that it leaves out obvious numbers that could be included with little effort may be deemed unreasonable. The do-not-originate list may include

only: Numbers for which the subscriber to which the number is assigned has requested that calls purporting to originate from that number be blocked because the number is used for inbound calls only; North American Numbering Plan numbers that are not valid; Valid North American Numbering Plan Numbers that are not allocated to a provider by the North American Numbering Plan Administrator; and Valid North American Numbering Plan numbers that are allocated to a provider by the North American Numbering Plan Administrator, but are unused, so long as the provider blocking the calls is the allocatee of the number and confirms that the number is unused or has obtained verification from the allocatee that the number is unused at the time of blocking.”

The Provider will ensure that regardless of what role it plays in the call chain, it will bar customers that have been found to be engaged / facilitating robocalls. Such as those that have refused to cooperate with its robocall mitigation efforts, as well as those that have been flagged as engaging in / facilitating robocalls based on its analytics data. This policy would be applicable to both new and renewing customers, to prevent them from originating or passing illegal calls through the Provider. In terms of the know your upstream provider rules, the Provider would apply the know your upstream provider steps described on this plan (such as those on page 3). As to the specific call analytics systems that the Provider uses to identify and block illegal traffic, the Provider may use a combination of its own proprietary systems (ex: analytics on switch software), software from cloud providers, software that comes with the switch/server equipment that it uses, data from its other providers in the call chain as well as data provided by its Certificate Authority (STI-CA vendor).