

Hotwire Telecom Inc. (Robocall Mitigation Plan)

This Robocall Mitigation Database (RMD) plan was prepared based on the FCC requirements listed on <https://www.federalregister.gov/documents/2023/06/21/2023-12142/call-authentication-trust-anchor>

(I). Status of STIR/SHAKEN Implementation

Hotwire Telecom Inc. fully implemented the STIR/SHAKEN authentication framework across its entire network using an FCC and iConnectiv approved STIR SHAKEN vendor. Hotwire Telecom Inc. 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

Hotwire Telecom Inc. uses software to monitor Hotwire Telecom Inc.'s 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 Hotwire Telecom Inc. if it originates any calls where the calling number is invalid, unallocated. If Hotwire Telecom Inc. determines that the caller was attempting to originate unlawful robocalls, then Hotwire Telecom Inc. can either warn them to stop or terminate their service as appropriate.

(III). Know Your Customer

For each call, Hotwire Telecom Inc. determines the nature of the business of each Hotwire Telecom Inc. customer, to ensure that the Hotwire Telecom Inc. customer is not providing services to those engaged in robocalling. Traffic from Hotwire Telecom Inc. customers is monitored continuously for patterns of known abuse. Immediate action is taken in situations where it is deemed necessary to prevent illegal robocalling or other forms of fraud.

(IV). Traceback

Hotwire Telecom Inc. 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 Hotwire Telecom Inc.

(V). Robocall Mitigation Plan Updated February 2024

The following is provided by Hotwire Telecom Inc. (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 headquartered voice service provider that directly serves US based end users making US Intrastate and US Interstate calls. It is just an originating carrier that serves end users in the US, and it is not an intermediate provider / wholesale provider. It is also not a non-gateway intermediate provider, nor does it handle any Int’l traffic and it is not a point of entry for foreign calls into the U.S. The Provider properly ensures the proper caller ID information when it passes a call to the next carrier in the chain. It also ensures that it properly signs calls = places its STIR/SHAKEN token for attestation in the SIP header of the call before it passes the call to the next carrier in the chain. The Provider will require the FCC mandated Caller ID data has been included when it receives a call. Also, it will ensure that the Provider passing the call to it has attested the call with STIR/SHAKEN token in the SIP header before the Provider passes the call to the end users it serves. The Provider will fully respond within 24 hours to all traceback requests received from the Commission, law enforcement, and the industry traceback consortium. In contracts with other Providers, the Provider will include language to require 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 Providers to provide the Provider with data needed to perform Due diligence necessary to understand the sources of the traffic being sent to it.

(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 will review the STIR SHAKEN technical standards. It will review FCC mandated 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 providers that are not in the Robocall Mitigation Database. The Provider will comply, and block traffic received directly from all 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 providers trying to send traffic to the Provider are on the Robocall Mitigation Database. Before those 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 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. As stated on page 1, The Provider does not play more than one "role" in the call chain. The Provider only has the role of directly serving end users in the US that are making US Interstate and US Intrastate calls. It is not intermediate carrier, wholesale carrier, gateway provider or non-gateway provider. The Provider will take the reasonable robocall mitigation steps (ex: required call ID and STIR SHAKEN token attestation). As described on page 2.

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. Though the Provider is not a Gateway 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.), if the Provider ever serves as a Gateway provider in a call chain, 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 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. 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).