AIRESPRING STIR/SHAKEN FAQs
FREQUENTLY ASKED QUESTIONS

What is STIR/SHAKEN?

STIR (Secure Telephony Identity Revisited) and SHAKEN (Signature-based Handling of Asserted information using toKENS) is an industry-developed system that makes use of public key cryptography to provide assurance that certain information about the Caller ID transmitted with a particular call is accurate.

Why is STIR/SHAKEN being implemented?

STIR/SHAKEN will address unlawful spoofing by confirming that a call actually comes from the number indicated in the Caller ID, or at least that the call entered the US network through a particular voice service provider gateway. STIR/SHAKEN should reduce the effectiveness of illegal spoofing and allow bad actors to be identified more easily.

How does STIR/SHAKEN work?

Once an originating or gateway provider has implemented STIR/SHAKEN standards, it should sign, or attest to, all IP-based calls originating on its IP-based network or entering the network through its gateway by adding a SIP header containing specific information enumerated in the standards. This header is then transmitted with the call to the terminating provider, which authenticates the call using the header and the originating provider's public key to ensure nothing has changed. Providers can give full, partial, or gateway attestation to the calls they sign. Full attestation indicates the greatest certainty that the caller is authorized to use the number, while partial and gateway attestation indicate less certainty but do indicate where the call originated on the network.

Is STIR/SHAKEN an FCC requirement?

The FCC has requested that all major voice service providers implement these new standards. Furthermore, in the FCC's June 6th 2019 Declaratory Ruling and Third Further Notice of Proposed Rulemaking, they indicated that they would require voice service providers to implement the STIR/SHAKEN Caller ID authentication framework in the event that they have not met FCC Chairman Ajit Pai's deadline for doing so by the end of 2019.

Does the FCC have the authority to require such a change in the event the voice service providers have not met the end of 2019 deadline?

The FCC cites section 251 (e) which grants the Commission plenary jurisdiction over the North American Numbering Plan resources in the United States and the authority to administer numbering resources and provides the Commission the authority to mandate Caller ID authentication and specifically STIR/SHAKEN. When bad actors falsify or spoof the Caller ID that appears on a consumer's phone, they are using numbering resources to advance an illegal scheme. By permitting voice providers and consumers to identify when a Caller ID number has been spoofed, mandating STIR/SHAKEN would prevent North American Number Plan resources from being fraudulently exploited. Accordingly, they conclude that this section 251(e) provides them sufficient authority to adopt such rules.

AireSpring STIR/SHAKEN FAQs

Will my calls potentially be blocked if my underlying service provider doesn't properly authenticate my Caller ID using the STIR/SHAKEN framework?

The FCC is taking these additional steps to protect consumers from illegal calls and ensure the effectiveness and integrity of the STIR/SHAKEN Caller ID authentication framework by proposing rules to allow voice service providers to block calls based on Caller ID authentication in certain instances. They further propose protections to ensure that the most important calls are not blocked. The FCC believes that these changes will make it easier for voice service providers to block calls. This has the potential to help providers achieve $3 billion in savings for consumers without inadvertently blocking critical calls. The FCC also proposed a safe harbor for voice service providers that offer call blocking programs that take into account whether a call has been properly authenticated under the STIR/SHAKEN framework and may potentially be spoofed. This safe harbor would provide the service providers the ability to block calls that are likely to be illegal.

Where can I find more details regarding the FCC's June 6, 2019 Declaratory Ruling and Third Further Notice of Proposed Rulemaking?

Click Here to Learn More

What is AireSpring doing to support these standards?

AireSpring is working cooperatively with other industry companies and our equipment vendors to implement these new standards. Our network equipment will support the insertion of the newly required data in the SIP header and we will be able to provide the public key to the terminating provider so that they can authenticate the call.

Why use AireSpring Telephone Numbers (TNs) and/or DIDs?

AireSpring is ready for these new standards and will ensure that any calls that originate on our network using our TNs and/or DIDs can be authenticated by the terminating provider. The result will be to prevent them from blocking calls from your numbers due to inability to validate your Caller ID details.