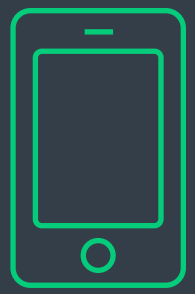
STIR/SHAKEN FAQs FOR CSPs

neustar®
A TransUnion® Company

Unwanted Calls Affect Everyone with a Phone Today.



Most distressing are calls where fraudsters hide their identity, by spoofing or changing the caller ID, to try to defraud consumers. To protect themselves, consumers don't answer unless they're certain who is calling.

Today, this issue is more than just a nuisance, it's a threat to public health and safety.

For businesses, that means their calls are not being answered and they can't relay important information to customers. New laws require that Communication Service Providers (CSPs) implement STIR/SHAKEN call authentication to stop fraudsters and restore trust in calls.

In our work to spread the word on STIR/SHAKEN, here are the top questions we've been asked by CSPs – along with answers from our team of experts.

FAQ 1

What Is STIR/SHAKEN?

STIR/SHAKEN is an industry-developed set of protocols and a governance model designed to stop the deluge of illegal robocalls to ensure the caller ID has not been spoofed.

STIR (Secure Telephony Identity Revisited) is a set of technical standards developed by the Internet Engineering Task Force (IETF) to certify the identity of originating calls. SHAKEN (Signature-based Handling of Asserted information using toKENs) is a framework developed by the Alliance of Telecommunications Industry Solutions (ATIS) that focuses on the implementation of STIR within IP-based service provider networks.

SHAKEN introduces a governance model that designates the roles and responsibilities of the Policy Administrator (STI-PA) and Certificate Authority (STI-CA) and outlines who is eligible to receive certificates (U.S. carriers with Operating Company Numbers [OCNs]).

It also defines additional data fields not included in STIR that enable traceback capabilities and a level of trust (attestation) based upon the carrier's relationship to the telephone number.

View our infographic on How STIR/SHAKEN works.

FAQ 2

How Does STIR/SHAKEN Stop Illegally Spoofed Calls?

STIR/SHAKEN establishes a trust chain between the originator of the call and the terminating carrier. If the chain is broken or the level of trust of the telephone number is low, it's a signal the call may have been spoofed, and the terminating carrier can decide how to treat the call—pass it to the subscriber, provide an alert to the subscriber, or block the call.

FAQ 3

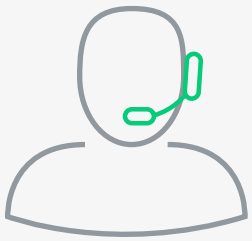
How Do Call Regulations Impact Communication Service Providers?

To address the surge in nuisance calls and voice fraud, Congress passed the TRACED Act in 2019, mandated that voice service providers introduce call authentication or a robocall mitigation program – at no cost to consumers. In March 2020, the Federal Communications Commission (FCC) adopted rules requiring providers to implement new standards based upon the STIR/SHAKEN standards. The TRACED Act mandated U.S. carriers implement STIR/SHAKEN call authentication measures or a robocall mitigation strategy by June 30, 2021.

In July 2020, the FCC also provided service providers with Safe Harbor when blocking calls that are likely illegal robocalls. This measure provides legal protection from liability when blocking suspected robocalls using reasonable analytics.

FAQ 4

Why Is STIR/SHAKEN the Best Solution to Stop Illegal Caller ID Spoofing?



STIR/SHAKEN is the most viable way to provide a measure of trust in the displayed caller name and number by authenticating the calling number with the identity of the caller. Today, the Terminating Service Provider (TSP) cannot tell if the number has been spoofed, which enables bad actors to pose as the IRS, banks, health care providers, or other.

STIR/SHAKEN brings together the cryptography that enables safe e-commerce with telephone security by providing an authentication mechanism to ensure a caller has the right to use a given telephone number. This best practice uses digital certificate to create a secure chain between the caller and recipient.

In the STIR/SHAKEN framework, digital certificates are typically issued to service providers, or in some cases others who are assigned dedicated telephone numbers. The private key associated with a digital certificate is used to sign a VoIP call, thereby indicating the calling party number has been properly attested.

The TSP uses the public key to unlock the message and ensures the message has not been compromised. The contents of the message are used by the TSP to determine call treatment and alerts to the subscriber.

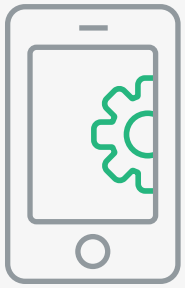
FAQ 5

What Types of Calls Does STIR/SHAKEN Address? How Will Non-IP Calls Be Handled?

Currently, STIR/SHAKEN focuses on calls that originate on VoIP (Voice over Internet Protocol). Standards are still being developed on how to address calls that make use of Time Division Multiplexing (TDM) switches. In the meantime, service providers are directed to implement a robocall mitigation program on the non-STIR/SHAKEN-enabled portions of their networks.

FAQ 6

How Are Calls Attested to with STIR/SHAKEN?



STIR/SHAKEN uses a system to categorize the essential information about the caller into three levels of "attestation." These attestation levels characterize a caller's level-of-trust of a particular number.

Full attestation, also known as "A-attestation," has several requirements but provides the highest level of confidence by the originating carrier. These calls must originate on the carrier's own network, as opposed to originating from another carrier or a VoIP provider. The carrier has also directly authenticated the caller and verified the caller's right to use the number. This will present challenges for some enterprises that have more sophisticated telephony implementations as some of their calls will receive a "B" level attestation. This creates an attestation gap that Neustar and others have developed solutions to resolve.

If the signing provider has not established a verified association with the telephone number or has no relationship to the initiator of the call (i.e., international gateways) the call will be attested at a "B" or "C" level.

Read the blog: Easy as ABC? Attestation Story Still Unfolding

FAQ 7

What If a Service Provider Has TDM in Their Network?

There are three key components to a service provider's network that determine the STIR/SHAKEN solution type:

- **Vendor interconnect** – connectivity to an upstream provider
- **Core network** – network equipment and infrastructure that provides signaling and transport
- **Last mile** – connectivity between the service provider and the customer

As long as the service provider is running SIP-enabled equipment, they can run an Out of Band (OOB) solution, which is similar to standard STIR/SHAKEN. The difference is that as part of the call, a token is also sent via the internet (OOB) that is separate from the call path. Even when the interconnect from the upstream providers is TDM, an OOB solution is still a viable approach to authenticating calls with STIR/SHAKEN. The last mile connectivity can be either TDM or VOIP and does not have an impact on a service providers ability to support STIR/SHAKEN.

For customers running traditional TDM equipment, a STIR/SHAKEN aware gateway is required to convert the signal.

FAQ 8

What Regions Have Adopted STIR/SHAKEN?

As of today, STIR/SHAKEN was mandated by regulators for implementation in the U.S. and Canada by November 2021.

Tier one carriers in the U.S. have already begun rolling out STIR/SHAKEN capabilities, well ahead of the June 2021 deadline, and leading Canadian operators are testing STIR/SHAKEN implementations.

As for other countries, a number of regulators in Europe, including Ofcom in the UK, are tracking the progress of STIR/SHAKEN adoption in the U.S. and are at various stages of developing initiatives in their own countries.

FAQ 9

What Should Service Providers Do to Implement STIR/SHAKEN?

Carriers were asked to take steps to implement STIR/SHAKEN by June 2021. Implementation of STIR/SHAKEN is a multi-step process that can take up to a year to complete. Participating in the STIR/SHAKEN ecosystem requires carriers to register and obtain SHAKEN digital certificates and credentials that enable them to sign all originating calls with the appropriate authentication information. Deployment of all the software services along with potential network upgrades are needed to automate the management of the certificates.

And, interoperability testing is highly recommended to work through any challenges and apply learnings to ensure success of your full-scale implementation of STIR/SHAKEN.

Get started with our CSP Checklist.

FAQ 10

What Solutions Are Available to Help Service Providers Implement STIR/SHAKEN?

Neustar, a TransUnion company, licenses Certified Caller, a complete solution suite, that includes all the required components to become compliant with the STIR/SHAKEN mandate. It can be deployed locally within a private cloud environment, or customers can access the product suite through our hosted service running in AWS. The software product suite supports both published REST and standards-based SIP proxy interfaces to the signing and verifying functions.

Neustar is a pioneer in call authentication, co-author of the IETF STIR standards, and contributor to the ATIS SHAKEN framework. We play a vital role in the governance structure for STIR/SHAKEN as an authorized Certification Authority in the U.S. and the Policy Administrator and Certificate Authority for Canada. We are at the forefront of the industry's quest to mitigate illegal robocalling and call spoofing.

The ATIS Robocalling Testbed, exclusively hosted by the Neustar Trust Lab, serves as the industry interoperability test facility to validate the effectiveness of caller authentication standards developed by the Internet Engineering Task Force (IETF) and ATIS.

Count on a Neutral Expert for Help.

The landscape continues to shift, so make sure you partner with a vendor that is staying abreast of the latest technical and regulatory changes.

As an approved Certification Authority and co-author of the STIR certificate management standards, Neustar plays an integral role in the governance structure for STIR/SHAKEN. We're at the forefront of the industry's quest to mitigate illegal robocalling and call spoofing. Learn more about our Certified Caller (STIR/SHAKEN) and Certificate Manager offering for service providers.

Visit our Trusted Call Resource Center to learn how STIR/SHAKEN is impacting your customers and how you can help them and see what resources and solutions Neustar offers.

EB-CSP-251635 02.11.2022

neustar®
A TransUnion® Company