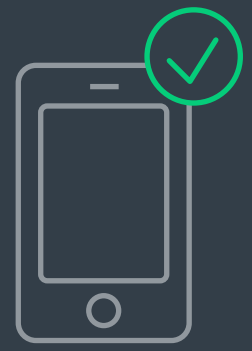
STIR/SHAKEN AND INBOUND CALLING

FAQs

neustar®
A TransUnion® Company

Reduce Phone Fraud with Neustar Inbound Authentication and STIR/SHAKEN



STIR/SHAKEN makes it harder for fraudsters to take over consumer accounts via call spoofing—a common tactic bad actors employ to attempt to impersonate customers. However, inbound call centers face multiple fraud vectors that revolve around the identity of the caller. That threat must be addressed by other analytics tools, without adding friction to the authentication experience. STIR/SHAKEN provides important signal into, but does not substitute for, inbound caller authentication solutions.

Discover how STIR/SHAKEN call authentication and inbound caller authentication combine to block out fraudsters while letting legitimate customers through faster.

FAQ 1

What is STIR/SHAKEN call authentication?

STIR/SHAKEN are technology standards that use certificates to digitally sign phone calls, a mechanism for communicating a calling number's legitimacy to prevent call spoofing. With STIR/SHAKEN, digital certificates are issued to carriers or other entities that own or are assigned dedicated phone numbers. A private key associated with each digital certificate is used to sign Voice over IP (VoIP) calls to indicate the calling party number's validity.

STIR/SHAKEN uses information about the originating caller to assign an attestation rating of A, B, or C to each call. These "ratings," set by originating carriers, indicate their relationship with the originator of the call and the network it originated from.

Depending on the call treatment algorithm used by service providers, customers will be notified with a symbol, verification keyword, or alert indicating that the incoming call has been validated. If the call cannot be verified, the carrier may block the call and/or alert the call recipient to a potential scam call.

Neustar, a TransUnion company, has been an integral partner in the long path to implementing STIR/SHAKEN: a co-author of STIR, contributor to SHAKEN, and the exclusive host of the ATIS Robocalling Testbed for validating STIR/SHAKEN implementations. As a result, Neustar is uniquely qualified to describe circumstances where STIR/SHAKEN is useful, and circumstances that require other solutions.

Read our eBook: STIR/SHAKEN Basics: What it means for your enterprise

FAQ 2

Are carriers required to implement STIR/SHAKEN?

The U.S. Federal TRACED Act and an order from the Federal Communications Commission (FCC) mandated that service providers implement STIR/SHAKEN call authentication and/or a robocall mitigation solution by June 30, 2021. Some carriers received extensions.

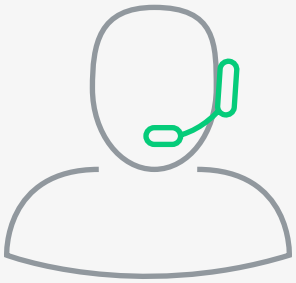
To ensure all carriers were participating and to uphold the quality of carriers' STIR/SHAKEN implementations across the telephone network, the FCC then created a Robocall Mitigation Database. Carriers must certify their actions around deployment of STIR/SHAKEN and/or a robocall mitigation solution in the database.

As of September 28, 2021, participating intermediate or terminating carriers must not accept calls from service providers that are not listed in the Robocall Mitigation Database. Carriers must provide periodic reports of compliance or risk ejection from the database.

Read our eBook: FCC Updates and Best Practices on STIR/SHAKEN

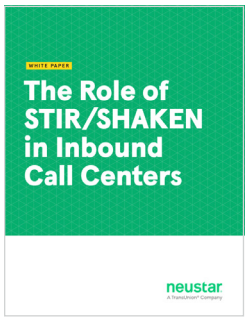
FAQ 3

Does STIR/SHAKEN protect inbound call centers from phone fraud?



STIR/SHAKEN can help inbound contact centers address fraudulent call spoofing—a common tactic bad actors employ to attempt to impersonate customers. However, call center leaders face multiple types of fraud that revolve around the identity of the caller. That threat must be addressed by other analytics tools.

In those cases, STIR/SHAKEN can serve as an important input. Adding STIR/SHAKEN data to existing call analytics tools provides incremental benefits.



Read our whitepaper: The Role of STIR/SHAKEN in Inbound Call Centers

FAQ 4

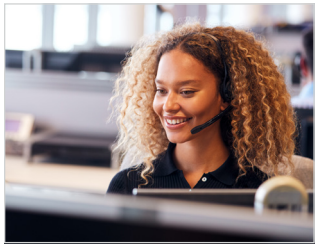
Will STIR/SHAKEN stop all phone-channel account takeover attempts?

No single approach can stop all phone-channel account takeover attempts. As STIR/SHAKEN improves detection of spoofed calls, fraudsters will likely adopt other phone-fraud tactics that do not rely on call spoofing. Of the phone-fraud vectors available—including burner or prepaid phones, unauthorized number reassignment, or other questionable activity—fraudsters will likely adopt virtual call services most frequently. Half of contact center leaders observed an increase of fraudsters using virtual call services to launch anonymous attacks in 2020. Virtual calls and spoofed calls differ fundamentally in technology and threat potential.

Skype and Google Voice are common applications in the virtual calling space, but they require some identifying information to create an account—a potential risk factor for some criminals. Hundreds of lesser-known virtual call services preserve anonymity during account creation.

These services allow criminals to place untraceable calls from anywhere in the world, ostensibly from any area code, while preserving anonymity. Worse, because calls from these apps are not spoofed, they may receive a high-level attestation. When a criminal reaches a call center agent from a legitimate number that is unrelated to a customer's record, they have an excellent chance of socially engineering the agent into granting control over a customer's account.

Forward-thinking enterprises are authenticating inbound callers' identities by inspecting their calls and calling devices. When the calling device is confirmed as authentic, and the Automatic Number Identification (ANI) matches the reference phone number on file, then the contact center can determine that it has engaged in an authentic call with the customer's unique, physical, legitimate phone – most often a mobile or landline phone. (This is identical to how credit cards facilitate cashless transactions.) If the caller's device is not unique and physical, then other signals can be used for a probabilistic risk assessment, such as calling history, call routing, line type, and STIR/SHAKEN attestation level.



Read: Not All Greens Are Created Equal

FAQ 5

What types of STIR/SHAKEN data will enterprises be able to obtain?

Inbound enterprise call centers can request the call verification status and/or the attestation level from their carriers or Neustar.

Verification status

A carrier-determined, binary pass/fail result that is designed to be passed to a phone where it could be presented as a check mark, verification keyword, or alert indicating that the incoming call has been validated. This can be sent to an enterprise but lacks the detail and original content of an attestation level.

Attestation levels

Attestations communicate three combinations of characteristics of the calling phone number: whether the caller is a customer of the carrier originating the call (the "originating carrier"), whether the originating carrier assigned the caller's phone number, and whether the call originated on the originating carrier's network.

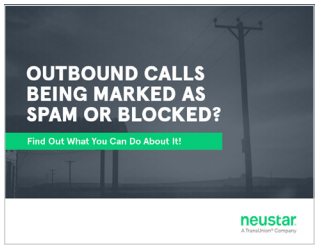
A. Full attestation. An A-level attestation conveys a strong level of trust. With this level, an originating carrier declares, "The caller is my customer. I gave him or her this telephone number. This call originated on my network." Spoofed calls should not receive an A- or B-level attestation.

B. Partial attestation. By assigning a B-level attestation, an originating carrier communicates, "The caller is my customer, and this call originated on my network. However, I do not know who assigned the number to the calling device."

C. Gateway attestation. In this case, the originating carrier is the entry point of the call into its VoIP network and has no relationship with the initiator of the call. This will often be the case with international gateways. A C-level attestation conveys, "This call originated outside my network." The call's phone number might be spoofed—a potential risk signal.

STIR/SHAKEN attestation levels provide an additional signal for identifying legitimate callers and determining treatment logic. Knowing how a call originated from the network is a useful signal of trust. A low-level attestation does not automatically indicate a threat—it just means that the call merits additional analysis. Many legitimate calls will receive B- and even C-level attestations.

To ensure customers get through as quickly as possible, and fraudsters get blocked, inbound call centers must be prepared to apply increasingly rigorous call analytics to all inbound call volume.



[Read the eBook: Outbound Calls Being Marked as Spam or Blocked?: Find Out What You Can Do About It!]

FAQ 6

How will enterprises obtain STIR/SHAKEN data to assess calls?

Carriers may only want to provide the verification status delivered to consumer phones. However, an attestation level is more valuable as it provides additional information for an enterprise than the verification status.

Email Neustar at callerid@team.neustar for help receiving full STIR/SHAKEN data in the SIP header of inbound calls.

Originating carriers encrypt the PASSporT—the "container" for the STIR/SHAKEN data in the identity header for the call. Terminating carriers use a verification service to validate and decrypt the PASSporT and provide the call's attestation level. Inbound enterprises may want to request the full, decrypted contents furnished by the verification service.

If a carrier is unwilling to provide a decrypted attestation, then enterprises can provide the encrypted identity header to Neustar Inbound Authentication.

Because Neustar provides a verification service for both carriers and enterprises, we can validate and decrypt the header, so that the attestation level can be added to the trust assessment of every call.

Read the eBook: STIR/SHAKEN FAQs for Enterprises

Treat Each Inbound Caller by Their Trustworthiness

Neustar Inbound Authentication establishes an optimal level of trust for each caller by combining a deterministic inspection of the caller's device with a probabilistic risk assessment of the call's signaling data, including the STIR/SHAKEN attestation level. Callers that pose a risk of third-party fraud are not deterministically authenticated in error, because they cannot manipulate or bypass the process.

As a co-author of STIR, contributor to SHAKEN, and the exclusive host of the ATIS Robocalling Testbed for validating STIR/SHAKEN implementations, Neustar occupies a unique position in the telecommunications industry to leverage STIR/SHAKEN data for inbound caller authentication. When an inbound call's header data includes an attestation level, Neustar Inbound Authentication can incorporate that data element in a probabilistic risk assessment.

FOR MORE INFORMATION ABOUT NEUSTAR INBOUND AUTHENTICATION

Call 1-855-898-0036 x4 | Email risk@team.neustar

Visit www.risk.neustar

FOR MORE INFORMATION ABOUT STIR/SHAKEN

Call 1-855-898-0036 x3 | Email callerid@team.neustar

Visit www.home.neustar/stir-shaken-resource-hub

EB-FRC-347513 01.12.2022

neustar®
A TransUnion® Company