

Mind the Gap.

The Impact of STIR/SHAKEN Attestation

STIR/SHAKEN Will Help Detect Call Spoofing and Decrease Fraudulent Calls.

The FCC's [June 30, 2021](#) STIR/SHAKEN implementation deadline has come and gone. But the impact on enterprises will hang around for a long time.

As more service providers implement the framework, there's a greater risk that legitimate business calls that originate with carriers that have not deployed it won't receive the highest attestation level and will fall into what is being termed the "attestation gap."



What's STIR/SHAKEN?

The TRACED Act mandated that all Communications Service Providers (CSPs) implement STIR/SHAKEN as the caller ID authentication framework in the Internet Protocol (IP) portion of their networks by June 30, 2021.

STIR [Secure Telephony Identity Revisited](#)

SHAKEN [Secure Handling of Asserted Information Using Tokens](#)

Ironically, as the industry works out the kinks in the STIR/SHAKEN rollout, legitimate calls may get marked as spam or blocked; consumers won't trust the call, and they won't pick up. Instead of increasing trust in the phone, it may decrease trust.

It's more important than ever for Communications Service Providers (CSPs) to carefully assess how call attestation levels are impacting their valuable enterprise customers.

And, enterprises must understand what options they have to ensure outbound calls are signed consistently with the highest appropriate attestation level.



Attestation: a Multi-Step Process.

STIR/SHAKEN uses vital information about the originating caller to determine an “attestation” level for the call – A, B, or C. These attestation levels are flags set by Originating Service Providers (OSPs) indicating how confident they are that the outgoing call is being made by the actual owner of the number – the call is not being spoofed.

The STIR/SHAKEN framework outlines the following process:

STEP 1

The Originating Service Provider (OSP) digitally assigns an attestation rating to a call, indicating whether they have authenticated the right of the caller to use the phone number, using these three criteria:

- Do I have a direct business relationship with this customer?
- Did I give the telephone number (either from my block or a TN leased from another carrier) to this customer?
- Did the call originate from my network?

Based upon the answers to these questions, the OSP assigns a commensurate attestation level.

STEP 2

Often, a call will pass through multiple carriers (transit carriers) before it reaches the called party's service provider. These carriers pass authenticated traffic without modification.

STEP 3

The Terminating Service Provider (TSP) uses a decryption key to validate the call has not been tampered with and then determines call treatment based upon analytics and the attestation level.

STEP 4

Depending the call treatment algorithm used by the service provider, the recipient of the call will be notified with a symbol, verification keyword, or some form of an alert indicating that the incoming call has been validated.

A = FULL

The OSP has the highest level of confidence in the caller. The OSP has verified the caller's right to use the number and origin of the call.

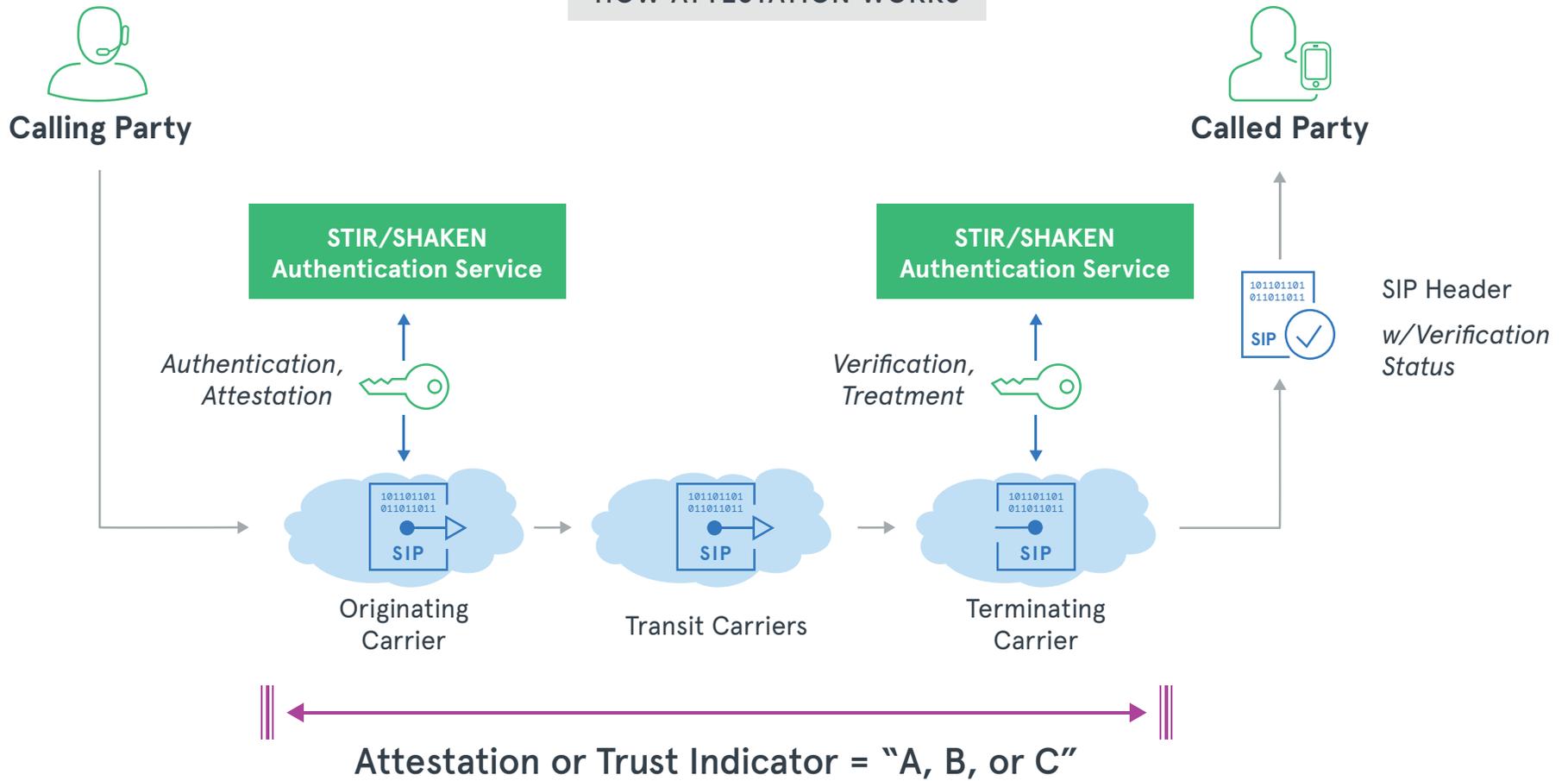
B = PARTIAL

The carrier knows the caller's identity but hasn't verified the right of the caller to the calling number. The originating carrier has no verifiable relationship with the phone number.

C = GATEWAY

Usually assigned to calls received from an international gateway or legacy systems. While service providers can determine where the call came from, they can't authenticate the caller ID or the caller's right to use the originating phone number.

HOW ATTESTATION WORKS



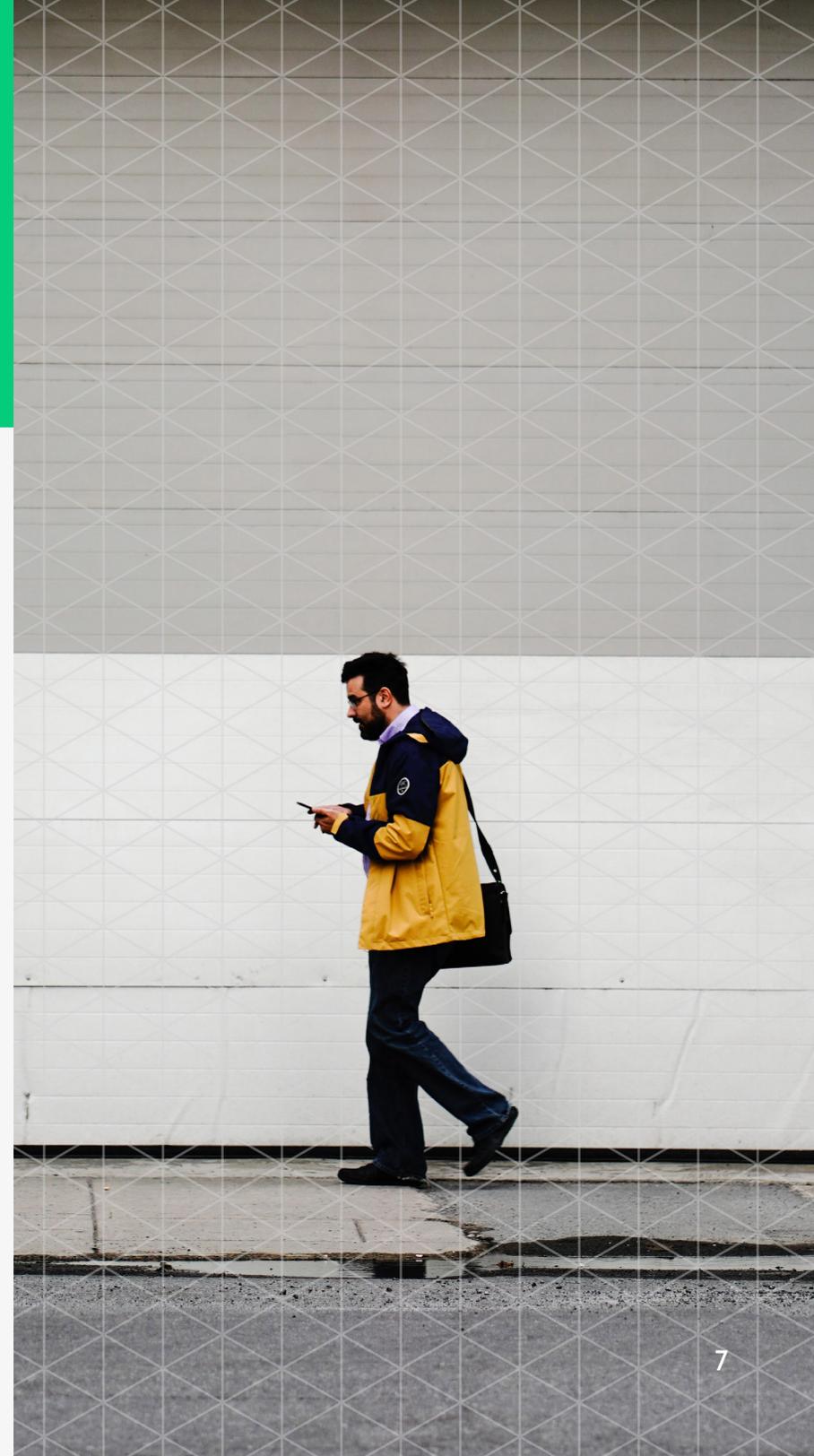
If the attestation level for the call is not an "A" or the call can't be verified, the TSP may block the call and/or alert the called party to a potential scam call.

It Gets Complicated with Multiple Service Providers.

Enterprises that get their phone numbers and voice services from a single carrier are likely to receive an “A” attestation because the originating carrier is certain of their identity, the source of the number, and originates the call on their own network. But there are many cases where calls are falling through the cracks.

Below are some common use cases where a problem exists:

- Enterprises that outsource to contact center providers
- Contact centers and enterprises that receive number blocks from multiple carriers, and use Least Cost Routing (LCR) for outbound traffic
- Contact centers and enterprises who receive SIP trunks from carriers and manage their own numbers



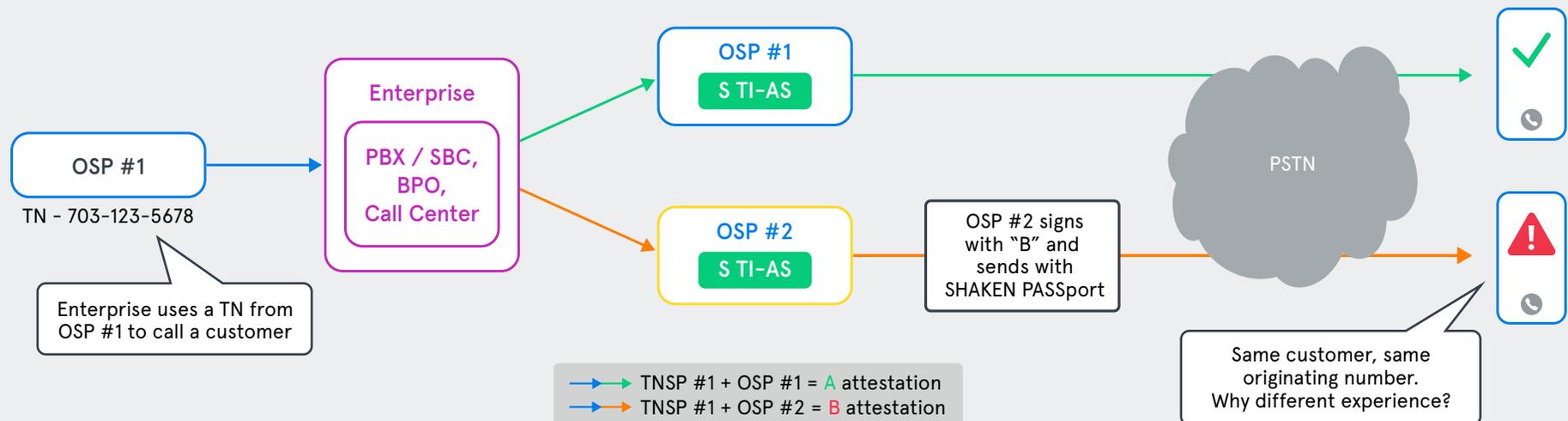
The diagram below shows an example in which an enterprise has obtained telephone numbers from multiple sources and has multiple service providers (OSPs). A common practice is for an enterprise to use the same telephone number and send calls to different trunks based upon costs, time of day, etc.

An enterprise call to the same consumer, using the same originating number, can have different results!

Attestation level is determined by combination of:

- Which carrier (TNSP) is the source of the phone number
- Which carrier (OSP) originates the call

Attestation Gap Creates Confusion



How to Get the 'A' in Attestation.

One way to resolve the attestation issue is for enterprises to authenticate their own calls using their own certificate(s). Unfortunately, most enterprises currently don't meet the requirements to obtain their own certificate, but they still want to ensure they receive an A-level attestation.

Several options exist to bridge the gap:

Name	Description	Status
OPTION 1: STIR Certificate	<ul style="list-style-type: none"> Vetted enterprise or carrier signs calls with STIR certificate; alerts OSP that the TN has been vetted 	<ul style="list-style-type: none"> Standard: based upon STIR RFC 8226 standard Industry adoption: tested in lab environment and ready to deploy
OPTION 2: Delegated SHAKEN Certificate	<ul style="list-style-type: none"> SHAKEN certificate is delegated from the Telephone Number Service Provider (TNSP) Vetted enterprise or carriers sign calls with SHAKEN certificate and can add rich call data 	<ul style="list-style-type: none"> Standard: approved by the PA but not deployed Industry adoption: tested in lab environment
OPTION 3: Telephone Number Database (TNDB)	<ul style="list-style-type: none"> Vetted TNs are stored and OSP signs using SHAKEN certificate Multiple flavors: local, centralized, federated 	<ul style="list-style-type: none"> Standard: limited progress formalizing standards-based approach Industry solution: local DB being deployed now
<div style="background-color: yellow; padding: 2px;">RECOMMENDED</div> OPTION 4: Sign Your Own Calls	<ul style="list-style-type: none"> Sign calls (generate PASSporT) with a standard SHAKEN certificate 	<ul style="list-style-type: none"> Standard: must meet criteria outlined below Industry solution: can obtain a certificate through an STI-CA, such as the Neustar Certificate Manager service

OPTION 1

STIR Certificates – Available Now!

Until a certificate delegation standard is implemented and required by the Policy Administrator (PA), enterprises will need to work with their OSP (vendor providing telephone services) to agree on one of two STIR PASSporT delivery options. Once a call is initiated, there are slightly different call flow paths for the PASSporT, depending on the agreed OSP policy.

Currently, Neustar's recommended approach is for enterprises to work with their OSP to agree on one of two STIR PASSporT delivery options:

- OSP validates and consumes STIR PASSporT and re-signs with SHAKEN
- OSP validates and transmits STIR PASSporT to TSP along with the OSP's SHAKEN PASSPORT

OPTION 2

Delegated Certificates Pending Approval: 2021.

While the SHAKEN framework has proposed the Delegated Certificates approach to ensure enterprises receive proper attestation, Neustar anticipates that standard will not begin to be implemented until the end of 2021, after it's been approved by the PA, requiring the use of official PASSporTs. And, it will take significant time before there is large scale adoption.

At that time, enterprises will be able to sign their calls using a SHAKEN certificate, through one of these two options:

- OSP validates and consumes delegated SHAKEN PASSporT and re-signs with SHAKEN certificate
- OSP validates and transmits Rich Call Data PASSporT to TSP along with SHAKEN PASSporT

OPTION 3

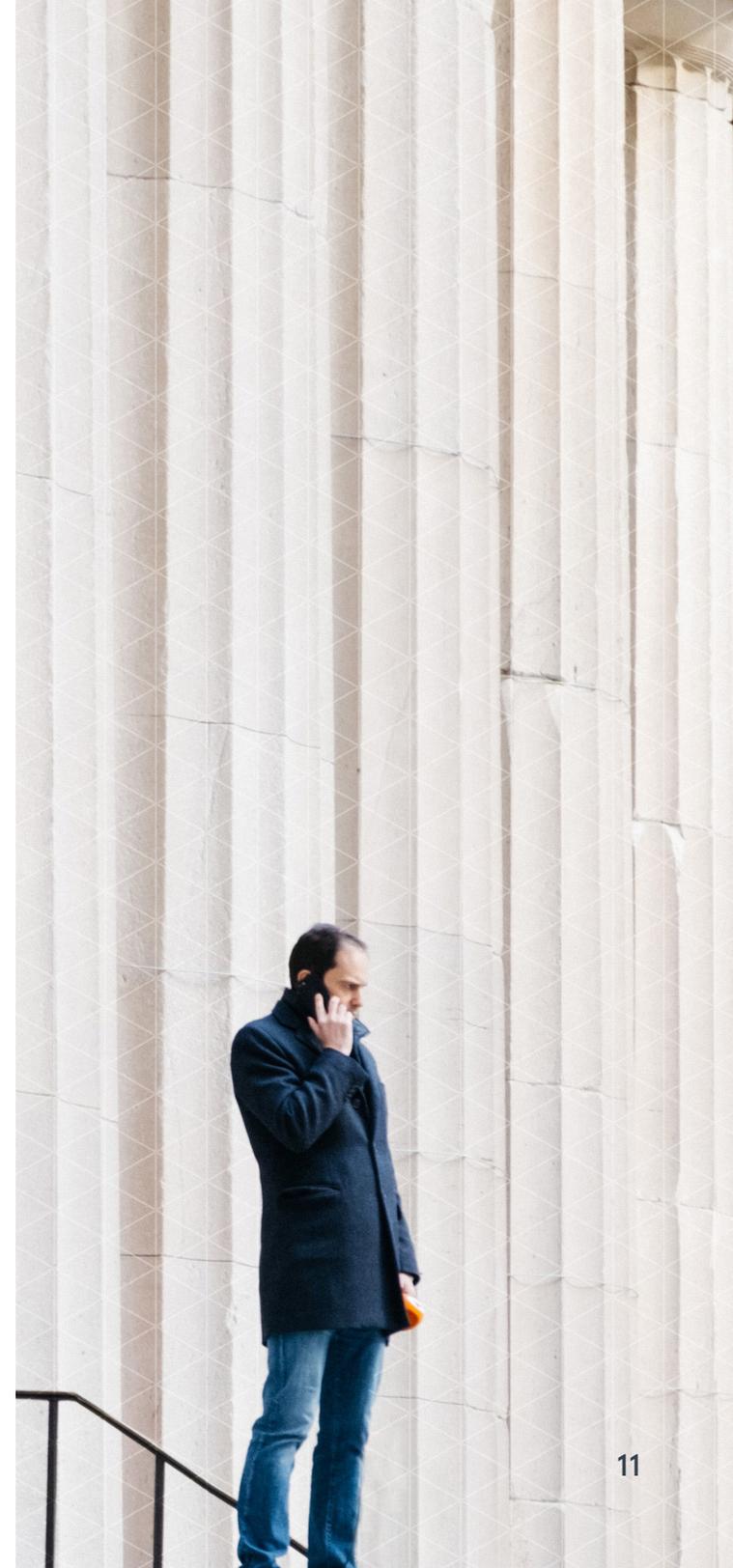
Telephone Number Database: Limited Traction.

A third prospective solution is the Telephone Number Database (TNDB), which acts as an authoritative source of TN-to-Enterprise association, including delegated authority by enterprises (e.g., to call centers). For the telephone numbers and enterprises to become trusted, they must first be vetted by a trusted neutral third party like Neustar.

OPTION 4

Sign Your Own Calls.

New regulations that go into effect in 2021 will enable Communications Service Providers (CSPs) to obtain a certificate by substituting direct access to TNs with STIR/SHAKEN implementation, or Robocall Mitigation program certification.



There's More Enterprises Can Do to Control the Call Experience!

Whether your situation is simple or complex, there are steps you can take, including:



Understand the STIR/SHAKEN landscape and your business impact.



Investigate the use of [branded calling](#). Ensuring end-to-end authenticated calls further allows the presentation of pre-vetted rich call data to the mobile display to provide additional context, so recipients are reassured about who's calling and answer the phone. Research shows that early adopters of branded calling have improved answer rates on first-call attempts by over 56%.



Assess Certificate Delegation, TN-Database, and/or STIR Certificate options and determine which best aligns to your business needs.



Visit our [Trusted Call Center](#) to learn about the seven-step trusted call journey.



For others in the ecosystem to trust your calls and provide favorable treatment, enterprises should investigate [vetting](#), which is also outlined in CATA Working Group's [Best Practices](#).



Take our free [outbound calling assessment](#). You'll receive a custom report with scores that will point you toward specific actions and next steps your business should take to ensure your calls get through to customers.

About Neustar.

Neustar is a pioneer in call authentication as the co-author of STIR standards and early contributor to the SHAKEN framework, and we play an ongoing leadership role in defining industry standards with ATIS, IETF, and CRTC. We provide the industry's reference implementation of STIR/SHAKEN as the exclusive operator of the ATIS Robocalling Testbed, where real world STIR/SHAKEN implementations are being tested for interoperability, and Neustar leads the industry in commercial call authentication deployments. Visit our [STIR/SHAKEN Resource Hub](#) to learn about insights, resources, and solutions.

Contact us at callerid@team.neustar.

©2021 Neustar, Inc. All rights reserved. All logos, trademarks, service marks, registered trademarks, and/or registered service marks are owned by Neustar, Inc. All other logos, trademarks, service marks, registered trademarks, and registered service marks are the property of their respective owners.

EB-CSP-263719 06.29.2021

neustar[®]