TECHNOLOGY

The STIR/SHAKEN FAQ Guide

The Ultimate Resource Guide

Your **Questions**
Answered by our **Experts**

General & Background
Regulatory
Authentication & Origination
Attestation
Termination & Subscriber Experience
STIR/SHAKEN & Numeracle
Resources
Recommendations

Numeracle

GENERAL & BACKGROUND

Does STIR/SHAKEN stop all robocalls?

While STIR/SHAKEN will help identify the origin of harmful robocalls, it will not completely eliminate all illegal robocalls for good. It's important to note that not all robocalls are harmful. Many legitimate companies communicate all sorts of information via 'robocalls' especially automated communications such as appointment reminders, delivery notifications, school closures, etc.

While the STIR/SHAKEN framework allows authentication of calls between originating and terminating service providers, it is not a silver bullet solution. It cannot determine the illegitimacy or legitimacy of the intent of an incoming call. It cannot validate that an incoming call with an A-level attestation has originated from an actual phone number, which is not being 'made up' or stolen from a legitimate business, organization, or consumer.

It is the responsibility of the originating service provider to ensure the caller is authorized to use the calling number and, if so, apply the A-level attestation, which indicates that status. Because the signature of the signing service provider cannot be spoofed, they are putting their reputation on the line when they provide A-level attestation.

The STIR/SHAKEN framework cannot weigh in on whether the content of the call itself is potentially malicious or unwanted, making call blocking and labeling analytics relevant despite the framework.

What is BASE STIR/SHAKEN? How is it different than full STIR/SHAKEN implementation?

What was expected for the June 2021 deadline was the implementation of the Base STIR/SHAKEN, or STIR/SHAKEN Standard, which is targeted at the internet IP-based service providers (non-IP providers will not be implementing it) to address Enterprises.

This means a SIP infrastructure is needed to add the certificate to attest the call. It assigns a telephone identity to be attached to the SIP invite, which is then transported over the SIP network to the terminating service provider, who does the reverse. The certificate is then validated and signed by the relevant key that has been attested, and they can choose how to terminate the call.

GENERAL & BACKGROUND

How does STIR/SHAKEN stop illegally spoofed calls?

The absence of STIR/SHAKEN technology allowed bad actors to easily misrepresent themselves with impunity when illegally "spoofing" or hiding behind a falsely presented calling telephone number. STIR/SHAKEN should aid in successfully identifying service providers who permit the origination of such calls. STIR/SHAKEN technology adds a cryptographic signature to a call. Verifying that signature identifies and proves which service provider(s) signed the call. With the improved ability to trace back to the origination of illegal activity, STIR/SHAKEN can assist government and telecom entities' ability to identify and stop the source of the illegal robocalls.

However, it is impossible to guarantee illegal spoofers won't slip through the cracks and end up with a STIR/SHAKEN attested call. Illegal call spoofing may still occur and is not solved or fully protected by STIR/SHAKEN because it can happen at origination before the call gets to the signing provider. Then it is up to the service provider to decide if they have enough information to give it an A-Level Attestation certificate. They might (especially if it's a crooked carrier), which could result in an illegally spoofed number provided with a green checkmark and deemed a "verified" and "trusted" call. Since STIR/SHAKEN is a new technology still being tested out in the United States, it's still vulnerable to potential fraudulent activity.

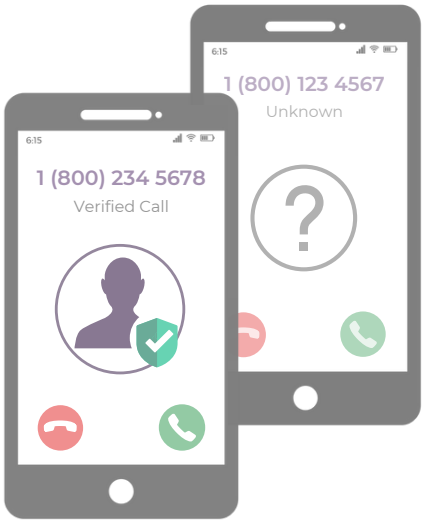
When calls are blocked, is an entity going to get notified that its calls are blocked?

When calls are blocked, is an entity going to get notified that its calls are blocked? This is still considered a bit of a mystery... When the call reaches its destination, the service provider has to decide if the call is an authenticated call or not. Analytics engines analyze aspects of the call for patterns like call volume, time of day, consumer-installed apps on devices that perform call blocking, originating IP, etc., to determine if the call is fraudulent, meaning you could get blocked due to other factors that may be at play.

Call blocking issues typically arise when businesses are originating calls and it's hard to determine where exactly those calls are coming from. Attestation information gets lost in the call path and terminating carrier analytics could potentially block the call. When this happens, there isn't a response sent to the originating provider notifying them that the call got blocked but there is an active discussion about introducing an error code transmission in the future.

GENERAL & BACKGROUND

My carrier completed STIR/SHAKEN, so why are my/my client(s) calls still being labeled?



External to the STIR/SHAKEN call authentication framework are 3rd party algorithms deployed at the wireless carrier level, known as call reputation analytics. These analytics have been deployed across mobile networks since late 2017 and are responsible for calls labeled as “Potential Spam,” “Spam,” “Scam,” “Scam Likely,” “Fraud Alert,” etc. that get assigned to phone calls at termination. Even if the originating provider signed the call with A-level attestation, the terminating provider may still label the call as ‘Spam.’

This could happen if the phone number itself is deemed as a number spamming consumers repeatedly, especially with short-duration calls, or if it was previously designated as a spammer before you used that number. These technologies will continue to deploy in parallel with STIR/SHAKEN, so if you’re hearing reports from your agents that your calls are ringing through as “Spam” or equivalent, this is due to reputational analytics, not STIR/SHAKEN.

While STIR/SHAKEN does aim to lessen the number of illegal robocalls originating and traversing the network, it does not filter for legal spam calls. STIR/SHAKEN call authentication seeks to achieve the identity verification status of the originating caller as a legal entity and the level to which they have the right to call using those numbers (Attestation Levels A, B, & C). STIR/SHAKEN may have verified your calls and identity, but this does not necessarily mitigate spam labels associated with your numbers. Your numbers could still get labeled as Spam or Nuisance based on various factors like aggressive or inconsistent dialing practices or consumer complaints. In a post-STIR/SHAKEN deployed world, you will still need to implement call blocking and labeling solutions to mitigate spam tags from associating with your numbers and brand.

REGULATORY

Whose responsibility is STIR/SHAKEN?

The logistics behind implementing STIR/SHAKEN do not fall to you but your telco provider. We recommend you keep pace with your service provider's progression toward STIR/SHAKEN implementation to ensure your calls will be given the greatest opportunity to be successfully authenticated.

With much still in the works behind the scenes with STIR/SHAKEN, it's also essential for you to voice your opinion and weigh in on the policies that will impact your business.

Be wary of solutions with 'guarantees' on STIR/SHAKEN, especially those with promises for 'enterprise signing' or 'attestation. It's impossible to predict exact outcomes with 100% certainty as the technology is in the early stage of widespread adoption.

What was the June 2021 STIR/SHAKEN Deadline?

As defined by the FCC in the TRACED Act, the June 2021 deadline required any provider of voice service to implement the STIR/SHAKEN authentication framework in their voice IP networks and required voice service providers to take reasonable measures to implement the effective call authentication framework (Robocall Mitigation Plan) in the non-IP portions of their networks.

The First Order mandated that it is the responsibility of originating and terminating voice service providers to implement STIR/SHAKEN Standards, or the Base STIR/SHAKEN, in the IP portions of their networks by June 30th, 2021.

Numeracle's Implementation Reports

Monitoring the Robocall Mitigation Database

1 June 30th - Sept 28th **2** Post-September 28th **3** Database Milestone

REGULATORY

Will my calls get blocked if I did not implement STIR/SHAKEN by the June 2021 Deadline?

Your calls will not be automatically blocked because of partial or incomplete STIR/SHAKEN implementation by the carrier network on which your calls terminate.

Call blocking and labeling analytics, however, will remain in place and continue to influence call treatment and delivery display on the terminating (device) side. If your calls are currently being labeled as "Scam" or "Fraud," they will still be able to be blocked as the result of this analytics and reputation-based classification, which occurs outside of the STIR/SHAKEN framework.

What was the September 28, 2021 Deadline?

This deadline was put in place to stop carriers from accepting and passing along any voice traffic that has either not implemented the STIR/SHAKEN framework or filed a Plan in the Robocall Mitigation Database.

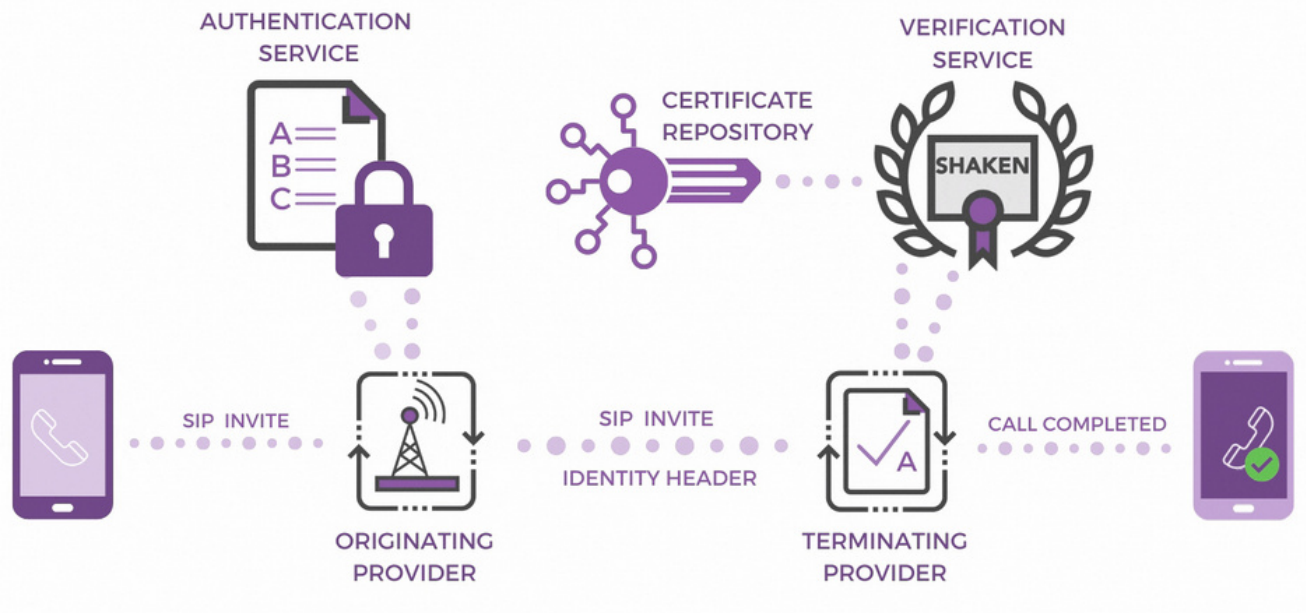
What are the top three points businesses should be aware of and should do to comply with STIR/SHAKEN?

In no particular order:

- Get an assessment of where your service provider is. You need to know what your service provider is doing, whether they're the BPO, the CPaaS, UCaaS, or the direct carrier, to comply with STIR/SHAKEN. Have they filed for an extension, or did they meet the deadline on time?
- Inquire how their compliance with the law will impact your current contract. Whether that results in an increase in cost or a service-level agreement change, you should be made aware of any contractual impacts on the services that they provide based on STIR/SHAKEN.
- Analytics will continue to exist to determine if calls are wanted or unwanted, legal or illegal. So you will still have to address your call blocking and labeling issues.

AUTHENTICATION & ORIGINATION

How STIR/SHAKEN works



What is Call Authentication?

Call Authentication is all about validating the identity of a caller by connecting the dots between the enterprise or contact center and its originating carrier(s) (telco providers) to ensure its calls are identified as trusted from the point of origination to termination.

Once the originating service provider has validated your identity as associated with your out-pulsed phone number (see: Numeracle's Verified Identity to learn more about this process), the next step is for the terminating device to authenticate the identity + phone number information passed from the originating service provider to display the call as a Verified Call (or not, if the identity + phone number can not be validated).

Who can sign my calls?

Only your telephone provider, CPaaS provider, or OSP can sign your calls.

AUTHENTICATION & ORIGINATION

Who is signing my calls with attestation levels? Who can give me a STIR/SHAKEN token or certificate?

The originating service provider placing calls and enabling the SIP invite into the network are signing calls with attestation levels via a STIR/SHAKEN token or certificate.

In most cases where the call originator or enterprise directly interacts with a carrier, like AT&T or Verizon, they originate and sign those particular calls. In cases where enterprises also have relationships with their reseller, the upstream originating service provider for that reseller is the one signing the call even though the enterprise is calling through a downstream provider/reseller.

The FCC recently required non-facilities-based service providers to register in the FCC's Robocall Mitigation Database, document and implement a robocall mitigation plan, register with the STI-PA, and authenticate calls using STIR/SHAKEN technology. In many cases, this means the VoIP provider must now comply. Check with your service provider to be sure.

What are the “Best Practices” for call authentication, and who wrote them?

Publicly available and at the request of the FCC’s Wireline Competition Bureau, the NANC, via its Call Authentication Trust Anchor Working Group (CATA Working Group), recommended the Best Practices. These practices attempt to outline how a service provider should accurately identify a caller and which aspects of a subscriber’s identity a provider should or must collect to enable it to verify the identity of a caller accurately.

ATTESTATION

What is Attestation?

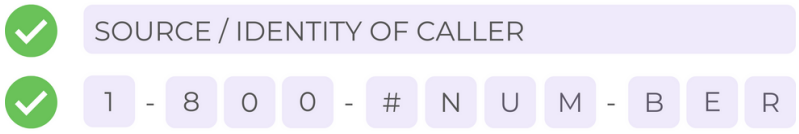
The term “attestation” in reference to STIR/SHAKEN refers to the level of certainty (defined in levels A, B, or C) the service provider has regarding the ownership or authorized use of the number being displayed in conjunction with the business’s identity.

When a STIR/SHAKEN call certificate is received, it will include a call’s Attestation Level, as signed by the originating service provider. This establishes the relationship with the caller and their right to use the calling number.

There are 3 Levels of Attestation:

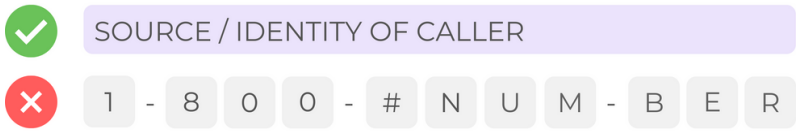
Full or Attestation “A”: the service provider knows the call source or identity of the caller as well as has the right to use that number.

Example: The carrier issued the number for a customer so the call originated in their network.



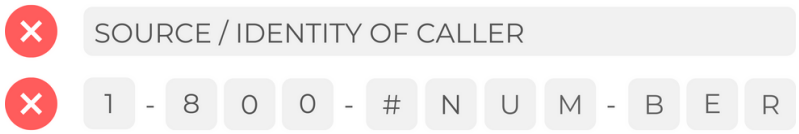
Partial or Attestation “B”: The service provider knows the customer, but not the source of the phone number.

Example: When third-party call centers are originating the call, the service provider may not know if they have the right to use that number.



Gateway or Attestation “C”: The service provider places the call into their network, but does not know who the originator of the call is.

Example: If a call originates from outside of the country and is coming through an international gateway.



ATTESTATION

How does Attestation Level translate to a call's trustworthiness?

The level of Attestation is not a direct correlation to the trustworthiness of the call.

Analytics will still be in place for call validation treatment to ensure that unwanted, scam or illegal calls will still be labeled accordingly. Attestation works to help establish the authenticity and identity of inbound callers but is not a substitution for call analytics solutions for call authentication.

What is the Enterprise Challenge?

One critical thing that goes on the STIR/SHAKEN certificate is the Attestation Level (A, B, or C). The gap occurs in complex scenarios like when a call center or BPO is making calls on behalf of multiple clients or where in some cases, there could be two or three parties involved in the call path. The end client could be someone who is not making the call but has outsourced the call to another call center that could use a different platform or CPaaS provider. In these scenarios, enterprises or service providers may be unable to validate the source or right to use the number to get their calls signed, known as the Attestation Gap.

Will A-Level Attestation guarantee that my calls will not be marked as 'Spam'?

A-Level Attestation comes in through the SIP network and terminates at the device. A-Level Attestation is one of many data points terminating providers consider when displaying a call.

Another data point taken into consideration comes at the analytics level, which is a separate layer outside STIR/SHAKEN Attestation and influences call display on mobile devices. These external analytics assess your phone number's reputation outside of the STIR/SHAKEN framework, which is where 'Spam' or 'Scam' labeling comes from.

A-Level Attestation does not necessarily influence the presentation of Spam or Scam labeling as the technologies are not currently integrated.

ATTESTATION

Can anyone guarantee A-Level Attestation?

An originating service provider could guarantee A-Level if they have a direct relationship with you as their client and have issued the numbers to you.

In any other situation, to facilitate A-Level Attestation, the originating service provider (OSP) needs a process to validate the enterprise in question's identity and validate that the phone numbers being used belong to that identity from whoever procured those numbers (if outside of the OSP).

Can less than A-Level Attestation be remediated or appealed or corrected?

It is unclear what the remediation process will be for calls signed with levels B or C. It will require a feedback loop to be put into place and techniques that still need to be defined based on the standards.

Is there a "Registry" or "Database" for callers to get A-Level Attestation? What is that, is it real, and is Numeracle a part of it?

Multiple models are currently being discussed to address Attestation and the Attestation Gap (Enterprise Challenge).

One proposed model is the centralized registry or database model, similar to a traditional CNAM database. This repository will store all the information related to numbers, including who owns the number, who has access to the number, or who is making calls on someone else's behalf.

Having this database would allow for retrieving any of this information. However, this is just one of the proposed models by the Standards Group. There are still questions about how this data is updated, who has access to it, who controls that access, or what happens if the database gets compromised.

ATTESTATION

From the carrier perspective, how does Numeracle act as a Local Policy solution for the service provider looking to ensure its clients' calls can be signed as A-Level Attestation, whether or not the service provider provisioned the phone numbers?

This can be validated through Numeracle's 'Number Profile' item within our Entity Identity ManagementTM platform. When a service provider needs to validate ownership of phone numbers provisioned outside the service provider, a request is sent to the entity to complete an LOA (Letter of Authorization) via a digital process, confirming the entity's authorization for authorization use of the phone number. That LOA is then used to form the baseline of truth for A-Attestation based on this authorized use of the phone number.

What happens when a call originator makes a call through a carrier with a number they acquired from another different carrier in regards to:
A) The level of attestation they can get?
B) If they do get a B level versus an A level, how will that impact what subscribers experience on the terminating side when called?

1. It depends on the carrier that is being used to originate the call. It comes back to the local policy they implemented and how they are treating that enterprise and that number. If the carrier believes they already know the customer/client/call originator and have a robust Know Your Customer (KYC) policy in place, it could theoretically be attested with A. However, a different carrier can take a different approach and always attest calls as B if the number was not acquired from them.
2. If it receives a B-level Attestation, thus far, we have not seen any difference between how the terminating carrier treats a B and A-Level as far as the presentation to the subscriber. As implementation continues, different visual displays such as a verification check may be used for only A-Level Attested calls.

ATTESTATION

Is there a way to test? How is it working so far?

Numeracle has clients using a provider that has implemented Base STIR/SHAKEN. We had them call our number to see how those calls were displayed, keeping in mind that our number is on one of the three major carriers. We found that the calls came through with the same display and appeared the same as calls from callers without authentication. This may be because the calls were given less than A-level attestation, or there may have been analytics, and local policy choices of Numeracle's service provider, which prevented Call Validation Treatment with "Verified" messaging and/or a green check mark displayed.

It also depends on the terminating service provider and how they accept call signatures. Call validation treatment and analytics will continue to play a role in the solution, and they are still on the network. How the actual call gets displayed on the device is based on how the terminating service provider does the CVT.

Attested calls currently do not show an attestation level, but we expect this will change over time as more begin implementing the standards.

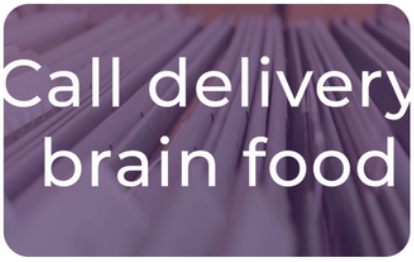
INSIGHTS BLOG

To learn more about our favorite topics related to call delivery, check out the Numeracle blog.

PODCAST

Your source of truth: live
Relevant and emerging topics in the telecom industry with industry experts.

OUR VOICE



Industry whitepapers, case studies, overviews, FAQ guides and co-authored thought leadership.

TERMINATION & SUBSCRIBER EXPERIENCE

How are “Verified” Calls displayed?

Some of the specificities around exactly how the "Verified" calls are visually depicted are still a work in progress, but the requirements to trace back to the identity of the caller are mandated by the TRACED Act and service providers are actively working to ensure they meet these requirements to avoid interruptions to service or calls blocked as the result.

Taking the steps now to ensure your identity is associated with the authorized use of your phone numbers to be verified (Verified Identity Certification) provides the Know Your Customer (KYC) evidence required to validate your identity to the service provider passing the STIR/SHAKEN signed call to termination, which will prevent the improper blocking of your calls and enable the highest levels of attestation (or authentication and visual depiction of the Verified status) possible.

What does “calls with a checkmark have been verified by the carrier” mean?

Calls that display a checkmark at the time of call or in the call history log represent that an originating service provider cryptographically signed the call, that the calling number was not changed during the call path, and that the call signature was verified via STIR/SHAKEN. Per the FCC’s recommended best practices, the caller's identity should have been vetted and validated so that you can trust that the caller is who they say they are and the number isn’t illegally spoofed.

However, you should be wary of the amount of trust placed in this verification mark because illegal call spoofing may still occur and is not solved or protected by STIR/SHAKEN because it can happen at origination before the call gets to the signing provider. Then it is up to the service provider to decide if they have enough information to give it an A-Level Attestation certificate. They might (especially if it’s a crooked carrier), which could result in an illegally spoofed number provided with a green checkmark and deemed a “verified” and “trusted” call.

Since STIR/SHAKEN is a new technology still being tested out in the United States, it’s still vulnerable to potential fraudulent activity. As much as we’d like to guarantee that calls with a verified checkmark can be trusted, there are exceptions where this is not the case, so it cannot be a guarantee (yet).

TERMINATION & SUBSCRIBER EXPERIENCE

What does a CNAM update accomplish?

When you update your CNAM with your phone company, they register this information in one or more CNAM databases where phone companies can access the data to display to their subscribers when you call them. Updating this information ensures its accuracy, as another person or company may have used a phone number previous to your usage or to correct any outdated information.

Are there any analytics around what percentage of phones will show a correct Caller ID Name after an update?

No. There are several CNAM databases that terminating service providers use. Even when CNAM is updated, until the database that a particular terminating service provider uses is updated, the Caller Name will not show the correct CNAM. Over some time, the databases sync with each other.

Who will see my updated Caller ID Name?

This depends on where the calls are delivered and if the Caller ID service is enabled for the end-user device. In most cases, the terminating service provider would use one of the CNAM providers to perform the Caller ID lookup. In some cases, the end-user might also have additional apps and services that could perform caller ID lookup.

NUMERACLE & STIR/SHAKEN

How does the Numeracle platform keep me/my client(s) in compliance with STIR/SHAKEN?

Numeracle's **Entity Identity Management™** platform allows an organization to manage its Verified Identity™ status as a legal business calling consumers based on an existing relationship or prior written consent. This verified status is governed by a compliance-based Know Your Customer (KYC) vetting process compliant with TRACED Act requirements and the TCPA. Our Platform also enables entities to identify the phone numbers used to engage with clients and subscribers and associate those numbers with Verified calling brands via "Number Profiles."

Will Numeracle's Entity Identity Management™ Platform take care of STIR/SHAKEN certification for me/my client(s)?

Not at this time, because the platform itself does not 'attest' or 'sign' calls, but the portal can gather and record the vetted identity and number information collected by us that helps protect phone number reputation and prevent improper labeling and blocking events. You can use the platform to implement a local policy solution for voice service providers to manage identity information and phone numbers to elevate the enterprise brand into the STIR/SHAKEN framework. You may have seen claims that solution providers can 'solve STIR/SHAKEN for you,' but this isn't entirely true because STIR/SHAKEN authentication is the responsibility of your voice service provider.

Verified Identity™

Establish your status as a Verified Identity™ through our compliance-based Know Your Customer process to vet and validate the legitimacy of your calling identity and establish trust in your brand.

TELL ME MORE

Number Reputation

Register phone numbers across wireless carriers & analytics partners via our online portal to monitor potential improper labeling, take corrective action to improve brand reputation, and lift contact rates.

TELL ME MORE

NUMERACLE & STIR/SHAKEN

What do I need to do external to Numeracle to fully comply with STIR/SHAKEN?

Your service provider must verify the relationship between your Verified Identity™ and authorized phone numbers (including optional rich call data for branded calling solutions) to enter them into the STIR/SHAKEN call authentication model.

You can find out from your service provider what kind of model they will be using to sign calls (i.e. Delegate Certificates, Centralized Registry/Database, Distributed Ledger Model), and what stage of development they are in. From there, we can work with them to ensure you comply with STIR/SHAKEN.

Should I be budgeting for some STIR/SHAKEN costs that may come into play?

It is going to depend on the service provider you are using and what costs they are going to associate with call signing.

One proactive approach would be to have this conversation with your service provider and ask if they're planning on passing along additional costs to facilitate call signing on their platform/network.

How does Numeracle help you fulfill your traceback requirements as a service provider?

The Numeracle platform can verify requests from the traceback group (run by US Telecom). The platform validates the identity of the entity and the authorized use of the entity's phone numbers.

RESOURCES

Follow evolving regulatory developments

ATIS IP-NNI Task Force

The IP-NNI Task Force, which Numeracle is a part of, is a co-author of the SHAKEN Standards.

Secure Telephone Identity Governance Authority

The STI-GA is a critical body helping the industry achieve the successful mitigation of unwanted robocalling.

Federal Communications Commission

Keep up with technology advancements

Join Numeracle on our bi-weekly Q&A sessions of Tuesday Talks, a live discussion series with hosts CEO & Founder **Rebekah Johnson** and Chief Product Officer **Anis Jaffer** that explores STIR/SHAKEN, emerging technologies' impacts to call delivery, enterprise identity, and more.

Listen to our past episodes here, available wherever you stream.
Register for our next session here.

RECOMMENDATIONS

Next Steps

- Understand what your service provider's requirements are and what method and local policy they are using to implement
- Understand the capabilities of your equipment and technology to display attested phone calls
- Be sure to implement before the June 30th, 2021 Deadline. If an extension is needed, have an implementation plan ready

REACH OUT TO US

CLICK