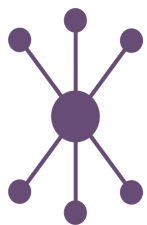




STIR/SHAKEN FAQ'S



Resource Guide: Your Questions Answered by our Experts

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



TABLE OF CONTENTS

General & Background 3

Regulatory 4 - 5

Authentication & Origination 6 - 7

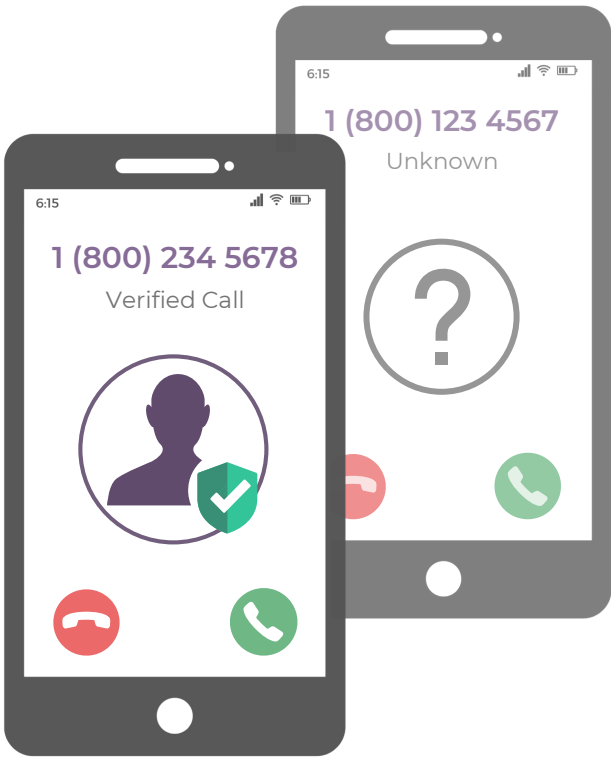
Attestation 8 - 11

Termination & Subscriber Experience 12 - 13

 RCD & CNAM 13

STIR/SHAKEN & Numeracle 14 - 15

Resources & Recommendations 16





GENERAL & BACKGROUND

Does STIR/SHAKEN stop all robocalls?

While STIR/SHAKEN will help identify harmful robocalls, it will not completely eliminate all illegal robocalls for good.

Not all robocalls are bad. 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 call originators and their numbers, it is not a silver bullet solution and cannot determine the legitimacy of the **intent** of an incoming call. It can validate that an incoming call is originating from a real phone number, which is not being 'spoofed' or stolen from a legitimate business, organization, or consumer.

The STIR/SHAKEN framework does not have the ability to weigh in on whether or not the content of the call itself is potentially malicious or unwanted, making **call blocking and labeling analytics** are still relevant despite the framework.

How does STIR/SHAKEN stop illegally spoofed calls?

The absence of this technology in the past allowed bad actors to represent themselves as someone they're not by illegally "spoofing" or hiding behind a falsely presented telephone number. With the improved ability to trace back to the origination of illegal activity, [STIR/SHAKEN will assist government and telecom entities' ability to identify and stop the source of the illegal robocalls.](#)



REGULATORY

Whose responsibility is STIR/SHAKEN?

The logistics behind implementing STIR/SHAKEN does not fall to you, but to your telco provider. We recommend you keep pace with your service provider's progression toward STIR/SHAKEN implementation so you can 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 very important 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.

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

Your calls will not be automatically blocked as the result 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.



REGULATORY

What is the September 28th, 2021 Deadline?

This deadline is 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 is Base STIR/SHAKEN? How is that different than the 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) 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.

What are the top three points businesses should be aware of and should do by June 2021 to be prepared for STIR/SHAKEN?

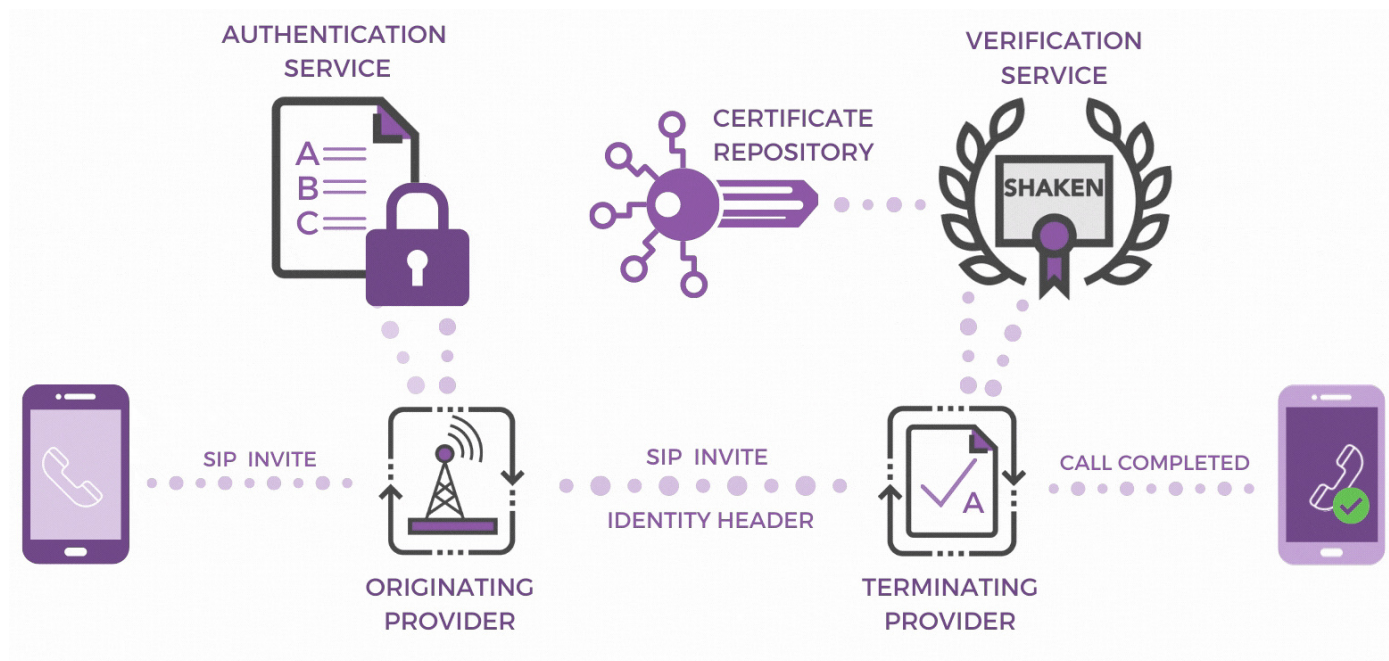
In no particular order:

-  Get an assessment of where your service provider is. You need to be aware of what your service provider is doing, whether they're the BPO, the CPaaS, or UCaaS, or direct carrier, to be in compliance with STIR/SHAKEN. Have they filed for an extension or did they meet the deadline on time?
-  Inquire how their compliance with the law is going to 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 are going to 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 in order 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 telephony provider, CPaaS provider, or OSP can sign your calls.



AUTHENTICATION & ORIGINATION

Who can give me a STIR/SHAKEN “certificate” or “token”?

The certificate that is being implemented by the network base SHAKEN framework will be hosted by the OSP. Enterprises will not have access to this.

In the delegate certificate model, you should be able to procure a certificate from a Certificate Authority but you may or may not be able to have that reside on your own infrastructure. The delegated certificates are an extension to the Base STIR/SHAKEN certificates. The standard and implementation of the delegate certificate model is a work in progress.

What are the “Best Practices” for call authentication?

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 should or must a provider collect to enable it to accurately verify the identity of a caller.



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 in regards to 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.




SOURCE / IDENTITY OF CALLER




1 - 8 0 0 - # N U M - B E R

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.




SOURCE / IDENTITY OF CALLER




1 - 8 0 0 - # N U M - B E R

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.



SOURCE / IDENTITY OF CALLER



1 - 8 0 0 - # N U M - B E R



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 authentication solutions.

What is the Enterprise Challenge?

One of the key things 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 be using a different platform or CPaaS provider.

In these scenarios, enterprises or service providers may not be able to validate the source or right to use the number to get their calls signed, which is referred to as the **Attestation Gap**.

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, in order 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 wherever those numbers were procured from (if outside of the OSP).

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

At this point, it is unclear what the remediation process will be for calls that are signed with levels B or C. It will require a feedback loop to be put into place and processes that still need to be defined based on the Standards.



ATTESTATION

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

Numeracle has a client currently using a wide provider that has implemented the BASE STIR/SHAKEN and 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. What we found was the calls came through as we would make any other calls without attestation.

It also depends on the terminating service provider and how they're accepting certificates. 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 CVT is done by the terminating service provider.

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

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 phone numbers were provisioned by the service provider?

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



ATTESTATION

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?

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

One of the proposed models is the **centralized registry** or **database** model which is similar to a traditional CNAM database. This repository will have all the information related to numbers stored, 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 the retrieval of any of this information, however, this is just one of the proposed models by the Standards Group. There are still questions around how this data is updated, who has access to it, and who controls that access, or what happens if the database gets compromised?

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?

A) 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.

B) 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.

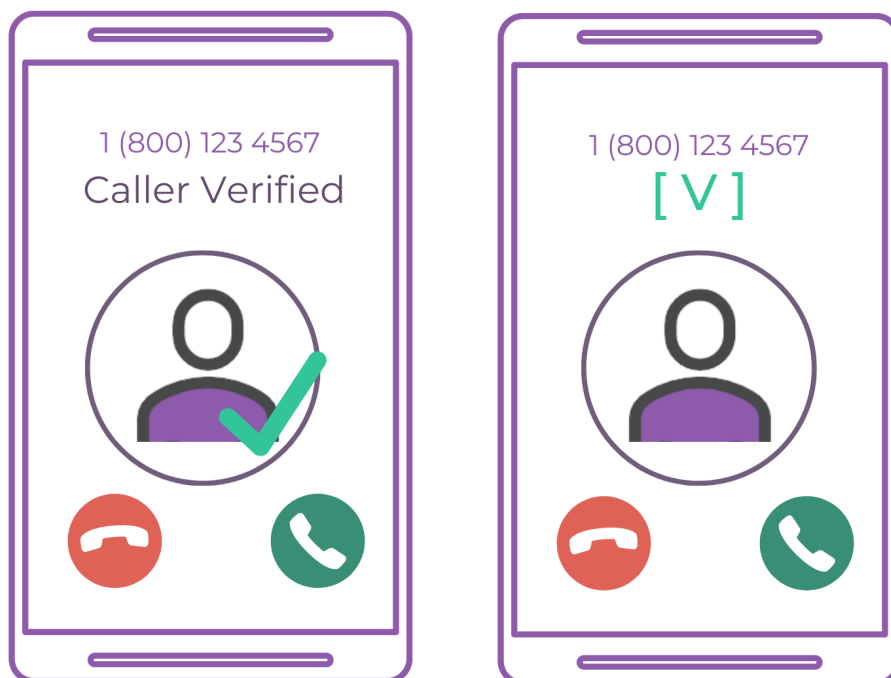


TERMINATION & SUBSCRIBER EXPERIENCE

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.





TERMINATION & SUBSCRIBER EXPERIENCE

RCD & CNAM

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 other phone companies can access the same information to display to their subscribers when you call them. Updating this information ensures its accuracy, as another person or company may have been using 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 ID will not show the correct CNAM. Over a period of time, the databases sync with each other.

Who will see my updated Caller ID Name?

This depends on where the calls are delivered to 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 Numeracle platform keep me 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 expressed written consent. This Verified status is governed by a compliance-based Know Your Customer (KYC) vetting process.

The Platform also enables entities to identify the phone numbers used to engage with clients and subscribers and associate those phone numbers to Verified calling brands via "Number Profiles."

This platform helps entities comply with STIR/SHAKEN by creating the authenticated relationship between Verified Identity™ and phone number usage, which is what service providers are required to verify in order to attest to the fact that each brand originating traffic on their network is authorized to use the phone numbers being displayed to the end-user.

Does Numeracle's Entity Identity Management™ Platform take care of STIR/SHAKEN certification for me?

While the Platform itself does not 'attest' or 'sign' calls, it can be used to implement a local policy solution for Service Providers to manage the verification of calling identity + authorization of phone numbers in order to elevate an enterprise brand into the STIR/SHAKEN framework.



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 will need to 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're in compliance 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?

Requests from the traceback group (run by US Telecom) can be verified by the Numeracle platform. 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 on [SoundCloud](#) & [YouTube](#)
[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](#)