The NobelBiz Guide for

STIR/SHAKEN for Contact Centers

nobelbiz®
Contact Center Technology

Table of contents

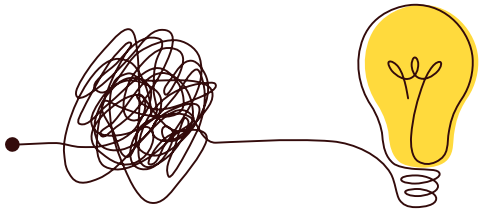
Introduction

This eBook is meant to provide all the necessary basic information to everyone who wants to understand what STIR/SHAKEN is, especially the professionals from the contact center niche. We will first look at the problem that preceded the implementation of STIR/SHAKEN, i.e. what is known as Caller ID Spoofing.

We are then going to see the evolution of the legal corpus that mandated the implementation of STIR/SHAKEN across the nation. Because this book is dedicated first and foremost to the contact center community, we will try to see how STIR/SHAKEN impacts the activity and performance of call centers or any type of businesses that are involved in outbound campaigns.

After we tackle the FUD and misconceptions surrounding STR/SHAKEN, we will jump straight into the why and how behind the two protocols. This will allow us to move to the last part of the eBook, which deals with the three levels of STIR/SHAKEN attestation.

Understanding the problem



Before we dive deep into the **whos, whats** and **hows** of STIR/SHAKEN, let's first clarify why there was a need for this in the first place.

The sad reality is that the contact center industry has a bad reputation for being a disruptive and intrusive piece of our social fabric. Unfortunately, the disruptive component is not even the worst part. Throughout time, our industry caught the headlines with many scandals, involving scams, identity theft, leaked data, and so on. It was only natural that these events would catch the attention of the legislators...

And technology plays a big part in this. With the emergence and widespread of VoIP systems, we saw an increasing number of robocallers and caller ID spoofing on the public telephone network. This type of spoofing was not possible on the previous landline technology.

To have a proper understanding of what Robocaller Caller ID Spoofing is and how it works we need to look at the three separate concepts that are into play: Caller ID, Robocalls and Spoofing.

What is the Caller ID?

Caller ID is a phone feature that, if available, displays the name and phone number of the person who is calling. Caller ID officially only provides the calling party's phone number, but its use as a word has effectively made it synonymous with the calling name as well.

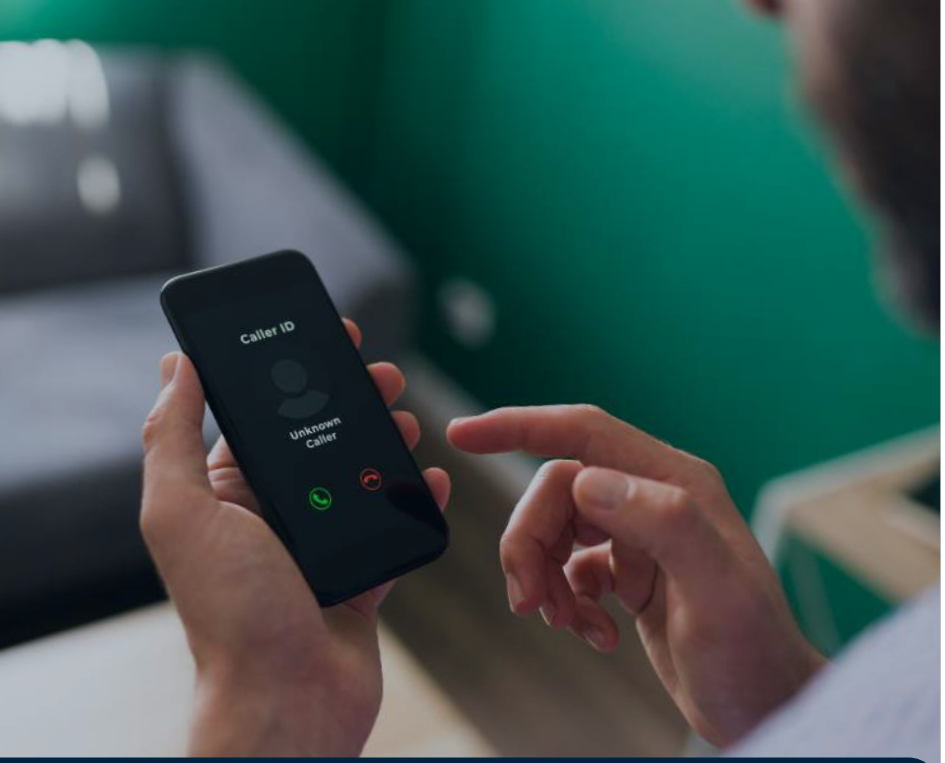
The calling party's name is really provided by a service called **CNAM (Caller Name)**. Caller ID can also be known as:

- *CID – Caller Identification*
- *CLID – Calling Line Identification*
- *CNID – Calling Number Identification*

Telephone provider companies often feature the Caller ID service for analog, digital and VoIP (Voice over Internet Protocol) phone systems.

According to Techopedia, Caller ID is one of two types:

- **Number Only:** Single Data Message Format (SDMF) is used, where the displayed information includes only the caller's telephone number and the date and time of the call.
- **Number Plus Name:** Multiple Data Message Format (MDMF) is transmitted, and the directory name is added to the displayed information.



> **According to the FCC:**
>
> ***…scammers often use neighbour spoofing so it appears that an incoming call is coming from a local number, or spoof a number from a company or a government agency that you may already know and trust. If you answer, they use scam scripts to try to steal your money or valuable personal information, which can be used in fraudulent activity.***
>
> *(Source: https://www.fcc.gov/spoofing)*

A Caller ID authentication technology such as STIR/SHAKEN allows customers to believe that callers are who they say they are, decreasing the efficacy of spoofing calls. This technology is essential for safeguarding Americans from robocall scams since it reduces callers' capacity to unlawfully fake a caller ID, which fraudsters exploit to mislead Americans into answering their phones when they should not.

Caller ID identification technology also makes it easier for customers and law enforcement to identify the source of unlawful robocalls, reducing their frequency and effect.

What is Spoofing? Legal vs Illegal Spoofing

Now that we know what a Caller ID is, we are ready to understand how spoofing actually works. Simply put, a spoof call is a call that changes (falsifies) the information that is passed on to the caller ID display of the receiving device.

The funny thing is that not all spoofing is bad or illegal spoofing. And here is where things get messy. To have a proper optics on what STIR/SHAKEN does, we need to know exactly what makes spoofing illegal.

There's a simple explanation for this: spoofing is illegal when it's against the rules set by the FCC. These rules change often and to prevent any damage to business activities, companies regularly need to check the FCC for updates.

The FCC defines illegal spoofing as spoofing done with the “intent to defraud, cause harm, or wrongly obtain anything of value.” Despite the vague language, this definition from the FCC is somewhat clear in that it reasonably eliminates all scammers and spammers. Telemarketing spoofed numbers are illegal if the numbers do not represent the company “on whose behalf the call is being made.”

EXAMPLES OF ILLEGAL SPOOFING:

Social Security imposters using a spoofed number to obtain social security information.

Healthcare scams where callers using spoofed numbers claim a relative of the person who is receiving the call is in the hospital and needs money for medical aid.

Tech-support schemes where callers impersonate tech companies and use numbers that seem similar to those of the tech firms.

In consequence, everything that does not fall under the FCC definition of what illegal spoofing is, qualifies as legal spoofing. If the number correctly represents the party who is making the call, if it is showing the name of the business as part of the caller ID, and if you can call it back, then it is legal, even if the number is spoofed.

To learn more about the difference between legal and illegal spoofing click here.

EXAMPLES OF LEGAL SPOOFING:

Medical professionals spoofing their number to display their office number so as to not reveal their personal phone number.

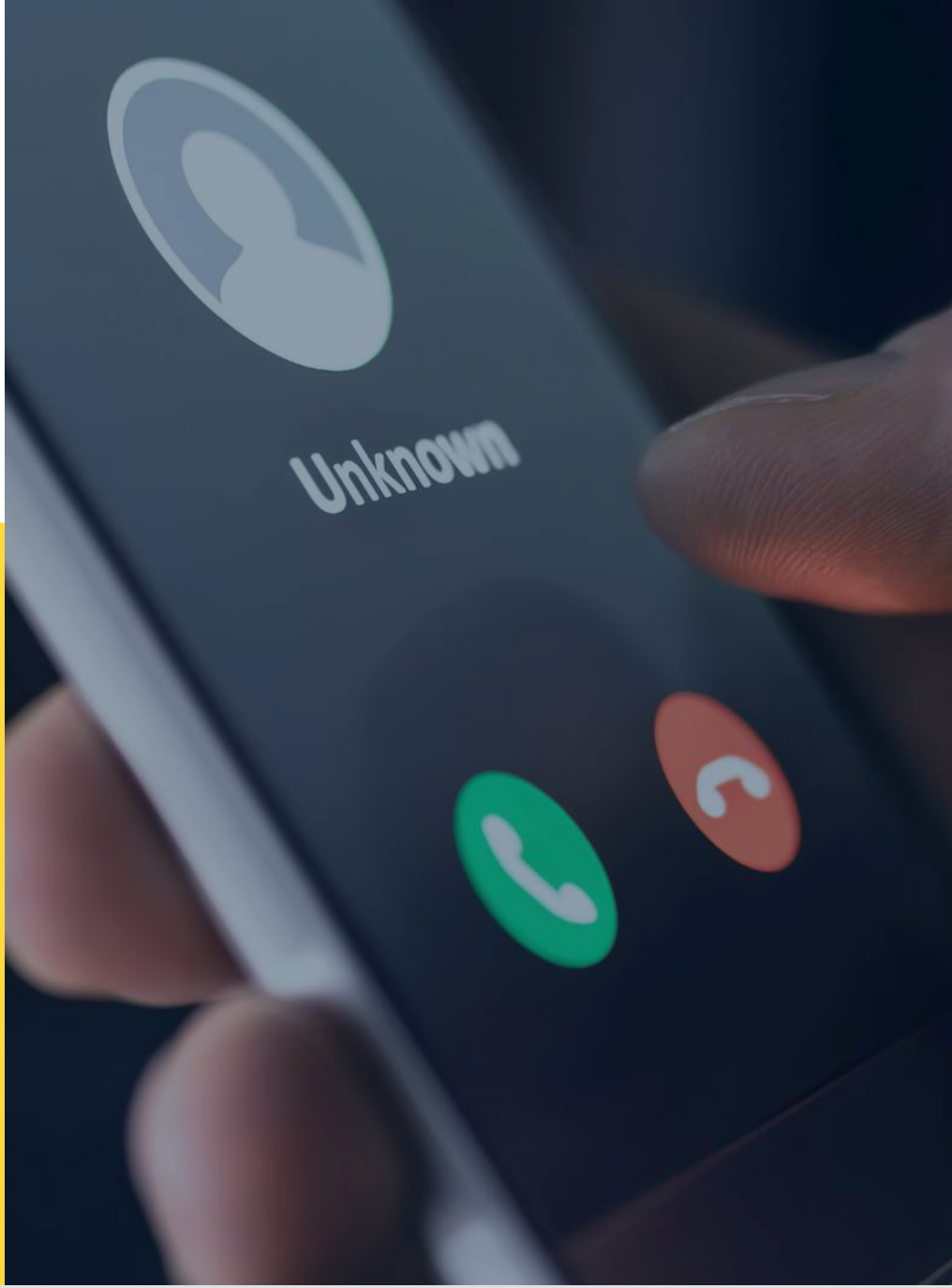
Telemarketers that call on behalf of a company or have the spoofed number associated with the company within the call ecosystem, and that have the same number available for callback.

Businesses that have toll-free numbers will often spoof all their numbers to display a toll-free one on the caller ID instead.

What are Robocalls?

In simple terms, every incoming call that has a pre-recorded voice message instead of a live person qualifies as a robocall. In general, for a robocall to be compliant with the FTC rules, the initiating company needs your permission before placing the call. However, there are a few exceptions from this rule. Robocalls can be initiated without the receiving person's pre-consent if they fall in one of the following scenarios:

- **Purely Informational Messages:** Robocalls about your flight being cancelled, events reminders, hazard alerts and so on.
- **Debt collection calls:** As long as they don't try to sell you services to lower your debt or other types of similar offers.
- **Political calls:** Endorsements, political messages and surveys, political event invites and so on.
- **Calls from some health care providers:** An example might be a robocall from a pharmacy or clinic reminding you about a recurring prescription.
- **Calls from charities:** As long as the charities are placing these calls themselves. If a third party is involved, unless you are a prior donor or member of the charity, the robocall is illegal.



Robocaller ID Spoofing

Now, let's put everything together and see what is the real reason why STIR/SHAKEN needed to be implemented and enforced: Robocallers and Caller ID Spoofing. Bad actors will always be one step ahead of the legislators, trying to speculate on emerging, unregulated technologies to achieve their end goals.

In this particular case, setting up massive automated outbound campaigns with pre-recorded messages that use misleading numbers to trick people into picking up the call.

According to the FCC:

> *"U.S. consumers received nearly 4 billion robocalls per month in 2020 … Unfortunately, advancements in technology make it cheap and easy to make massive numbers of robocalls and to "spoof" caller ID information to hide a caller's true identity."*

Looking for a solution: STIR/SHAKEN Legislation

Following a surge in consumer complaints about robocalls and telemarketing calls, the Federal Communication Commission (FCC) brought together an impressive group of tech companies to assemble the so-called “Robocall Strike Force”.

FCC’s Robocall Strike Force

• The first meeting of the Robocall Strike Force was held on August, 19th at FCC headquarters in Washington, D.C and in October 2016 the issued the first Robocall Strike Force Report. In his July 26, 2016 blog, Chairman Wheeler asked the industry to “develop an action plan for providing consumers with robust robocall-blocking solutions”. On August 19, 2016, a 60-day Strike Force was created to meet the Chairman’s request.

• The Strike Force created work groups to facilitate the collaboration across the telecommunications ecosystem. The work groups arranged around the four categories indicated below, and met at least twice per week over the last 60 days.

Strike Force Members

• The Strike Force was organized in 4 Work Groups: 1. Authentication 2. Empowering Consumer Choice 3. Detection, Assessment, Traceback, and Mitigation 4. Regulatory Support/Root Cause Removal.

• STIR/SHAKEN is featured as a solution for the Authentication Work Group, which had 16 meetings and 75 contributors:

The Strike Force accelerated, from December to October, the standards to verify and authenticate caller identification for calls carried over an Internet Protocol (IP) network. These standards are known as SHAKEN (Signature-based Handling of Asserted information using toKENs) and STIR (Secure Telephony Identity Revisited). The development and implementation of the standards after the 60-day term will continue through the Internet Engineering Task Force (IETF), Third Generation Partnership Project (3GPP) the Alliance for Telecommunications and Industry Solutions (ATIS) Session Initiation Protocol (SIP) Forum, and the IP Network-to-Network Interconnection Task Force.

• In July 2017, the Media Relations and Wireless Telecommunications bureaus of the FCC released a document called: ***FCC Seeks Reliable Call Authentication System***. In this document, the Commission acknowledges the problem of spoofed robocalls and asks for public comment on standards that will help differentiate legitimate phone calls from those that attempt to trick consumers through caller ID.

• In June 2019 the FCC issues the ***Advanced Methods to Target and Eliminate Unlawful Robocalls, Declaratory Ruling and Third Further Notice of Proposed Rulemaking***, *an item provides clarification voice service providers may use now to block illegal and unwanted calls before they reach consumers' phones, and proposes additional means providers may use in the future to block those calls.*

• At the end of March 2021, the FCC Mandates STIR/SHAKEN to Combat Spoofed Robocalls, i.e. an industry-wide deployment of STIR/SHAKEN:

• Today's Order requires all originating and terminating voice service providers to implement STIR/SHAKEN in the Internet Protocol (IP) portions of their networks by June 30, 2021, a deadline that is consistent with Congress's direction in the recently-enacted TRACED Act. The FCC laid the groundwork for these new rules when it formally proposed and sought public comment on mandating STIR/SHAKEN implementation in June 2019.

STIR/SHAKEN and the TRACED Act

On December 31st, 2019, after a decisive 417-to-3 House vote and a unanimous consent in the Senate, the Pallone-Thune TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act was passed into law by President Trump.

The TRACED Act requires businesses to implement the STIR/SHAKEN call authentication framework within 18 months and also make steps towards the implementation within 12 months.

On March 10th, 2020 the FCC came up with a framework for implementing the STIR/SHAKEN caller ID authentication protocols by June 30, 2021. The framework was voted on March 31st, 2020.

Access the full report on the FCC website

Read more about the TRACED Act

STIR/SHAKEN and the Contact Center Industry

At this point, we can hardly imagine there is a single person in the contact center industry that has not heard about STIR/SHAKEN.
Although implementing STIR/SHAKEN is something your telecom provider needs to worry about, if your company is making ANY type of outbound call, STIR/SHAKEN is on your menu, regardless if you like it or not.

Who needs to do What?

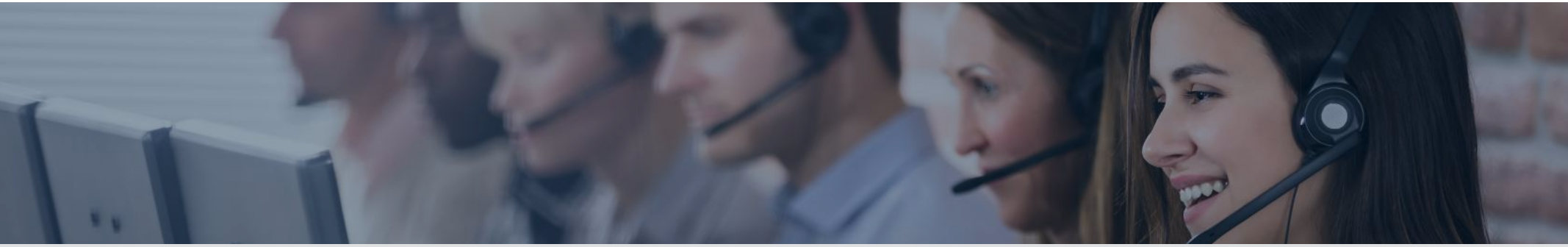
STIR/SHAKEN uses a technology and process to allow carriers to digitally sign calls and attest to whether or not the calls they are processing are coming from people they have a business relationship with and are using numbers that they have permission to use.

Alright, the good part of this overly simplistic explanation is that the carriers are the ones who need to worry about the technicalities of dealing with STIR/SHAKEN.

However, this doesn't mean that you can lay back and let your telecom provider do all the hard work.
You too have a role to play, in what level of attestation your calls will receive.

Because carriers can now be held accountable for the traffic and attestation they inject into the network, they will need to walk you through their internal process, explaining how they assign the three levels of attestation: A, B or C and where your calls fall under and in what situations.

Of course, for level A attestation, you, as a call originator, need to meet certain requirements. One thing you need to know before we move to the next section of the article is that every carrier has its own validation process. To learn more about the validation process of NobelBiz, get in touch with one of our experts.



Attestation Level Misconceptions

In theory, every call originator will want to have the highest possible attestation for his or her business. But this cannot be assumed especially when a company uses multiple carriers, uses numbers from their end clients, or relies on a UCaaS or CCaaS platform to deliver their calls. Here are a few of the most common misconceptions a call center owner or manager needs to be aware of:

1

Having your calls attested B or C does NOT automatically mean that your calls do not comply with the TRACED Act.

Having your calls signed and given a level of attestation in of itself is compliant with the TRACED Act. The level of attestation is what relationship, if any, the provider has with the call originator and knowledge of the ownership or permission to use the numbers as caller ID.

2

Levels B and C does NOT automatically mean your calls will be blocked or mislabelled as spam, scam or fraud.

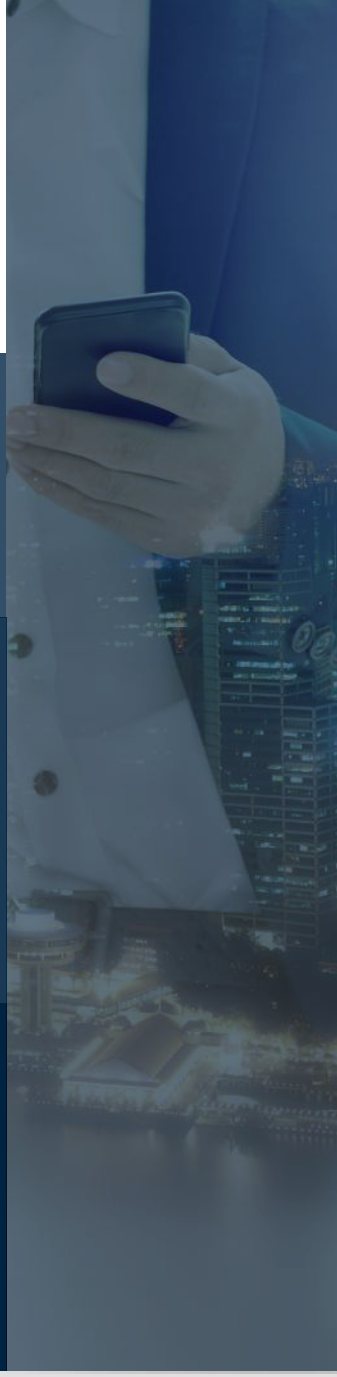
Today, calls are being mislabelled and blocked via different mechanisms and providers. Not all but some providers who block and label calls will use the information from signed and unsigned calls as one of many data points to make their decisions: everything from call frequency, average call duration, call attempts, complaints, blocks, short duration calls, and so on.

At this time there are no standards around how the level of attestation will impact what the subscriber sees on their device or how this would cause your calls to be automatically treated as fraud or scam.

3

STIR/SHAKEN will NOT solve your current problems with blocked or mislabelled calls.

A very common misconception is that STIR/SHAKEN will somehow magically solve all the problems with call labelling and blocking. Unfortunately, this is not true. As mentioned above, STIR/SHAKEN and Call Labelling and Blocking are not the same thing and do not rely on one another to work. They may influence one another, but having one does not mean the other will go away. Any issues you are having now or could have in the future will need to be addressed via other layered approaches, which Nobelbiz can help with.



Common Situations That Could Impact Attestation Levels

If you have questions or concerns about the items we outlined, NobelBiz can definitely help you with this.
Get in touch with one of our experts.

HAVING MULTIPLE CARRIERS

Having multiple carriers is normal for many companies for a variety of reasons. One thing that could impact your level of attestation in this scenario is when you begin to use numbers from one provider on another providers' network. Make sure to talk to your carriers and make sure to know what happens to your level of attestation under this situation. It is possible you could go from an A to B level attestation if you don't understand their local policy.

USING NUMBERS OWNED BY ONE OF YOUR CLIENTS

It is not uncommon for an outsourcer to use numbers their clients own as caller ID. Because the outsourcer does not own those numbers, it is important to discuss this use case with your provider or carrier as it could cause you to have a B level attestation. Make sure to understand your providers' internal policy.

USING A CCAAS OR UCAAS SOLUTION

More and more companies are moving to cloud solutions. These solutions have many advantages including not having to be a telecom expert and manage your carrier relationships if your provider does it for you. The one area you want to cover with your provider is how are they handling the following:

1) Is your provider signing your calls or is a 3rd party (like one of their carriers) signing the calls?
2) What happens when there are call quality issues and your provider changes who the carrier is? Does that impact how your calls are signed?
3) Will there be multiple downstream carriers in route for your calls and will all of them be consistent in attestation or delivery of calls?

What is STIR/SHAKEN?

The STIR/SHAKEN framework is an industry-standard caller ID authentication solution that consists of a set of technical standards and protocols that enable the authentication and verification of caller ID information for calls made over Internet Protocol (IP) networks. This was devised to combat all kinds of spoofed calls and to tackle the problems that we've discussed in the first part of this eBook.

We've seen that Caller ID masking is a form of spoofing use by robocallers for nefarious reasons by tricking people into thinking they are receiving calls from a local or legitimate entity. With the advent of the voice-over-IP telecom systems, this type of spoofing started to be more and more prevalent.

STIR/SHAKEN allows the originating carrier to generate a digital signature that securely signals the caller's right to use a phone number to the terminating carrier. STIR/SHAKEN offers a practical mechanism to provide verified information about the calling party as well as the origin of the call — what is known as "attestation."

When you make a call, your phone carrier will use your identifying number to create a digital signature, or token, that will accompany the call as it is being completed.

The Alliance Telecommunications Industry Standards (ATIS) has developed three key standards that form the basis of STIR/SHAKEN:

- *ATIS-1000074 - Secure Handling Of Asserted Information Using toKENs (SHAKEN)*
- *ATIS-1000080 - Secure Handling of Asserted information using toKENs*
- *(SHAKEN): Governance Model and Certificate Management*
- *ATIS-1000084 - Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators.*

At the other end, the system verifies that nothing was tampered with, ensuring that the call came from someone with a legitimate right to use that number.

As implementation progresses, Americans will have more confidence that the caller ID information they receive is correct, and voice service providers will be able to provide useful information to their customers about which calls to answer.

STIR

Secure Telephony Identity Revisited

is a call-certifying protocol developed by the Internet Engineering Task Force (IETF) to authenticate telephone calls end-to-end.

SHAKEN

Signature-based Handling of Asserted information using toKENs

What is STIR?

STIR is a very flexible protocol that can be implemented in many ways, including the end user installing client software, obtaining a personal "key," and proactively managing the process of keeping software current and regularly renewing keys. This is beyond the capability of most users today, but the flexibility in the protocol also allows STIR to be implemented in other ways, including within the service provider network. Unfortunately, this flexibility can also create problems. When a protocol has too many options and independent implementations inevitably make different choices, they "won't play nice together" and a call from one service provider won't be successfully verified by a second service provider.

This is where SHAKEN comes to the rescue by precisely specifying implementation details. SHAKEN specifies a "profile" of the STIR protocol; STIR defines how you could implement the protocol, while SHAKEN documents how you will implement the protocol.

What is SHAKEN?

According to a document created by the Alliance for Telecommunications Industry Solutions (ATIS), SHAKEN (Signature-based Handling of Asserted information using toKENs) was developed by the ATIS-SIP Forum IP-NNI Task Force. IP-NNI stands for "Internet Protocol - Network to Network Interface." SIP stands for Session Initiation Protocol. SHAKEN is based on the STIR (Secure Telephone Identity Revisited) protocol – essentially, SHAKEN defines a profile of the STIR protocol, which is why it is typically referred to as STIR/SHAKEN.

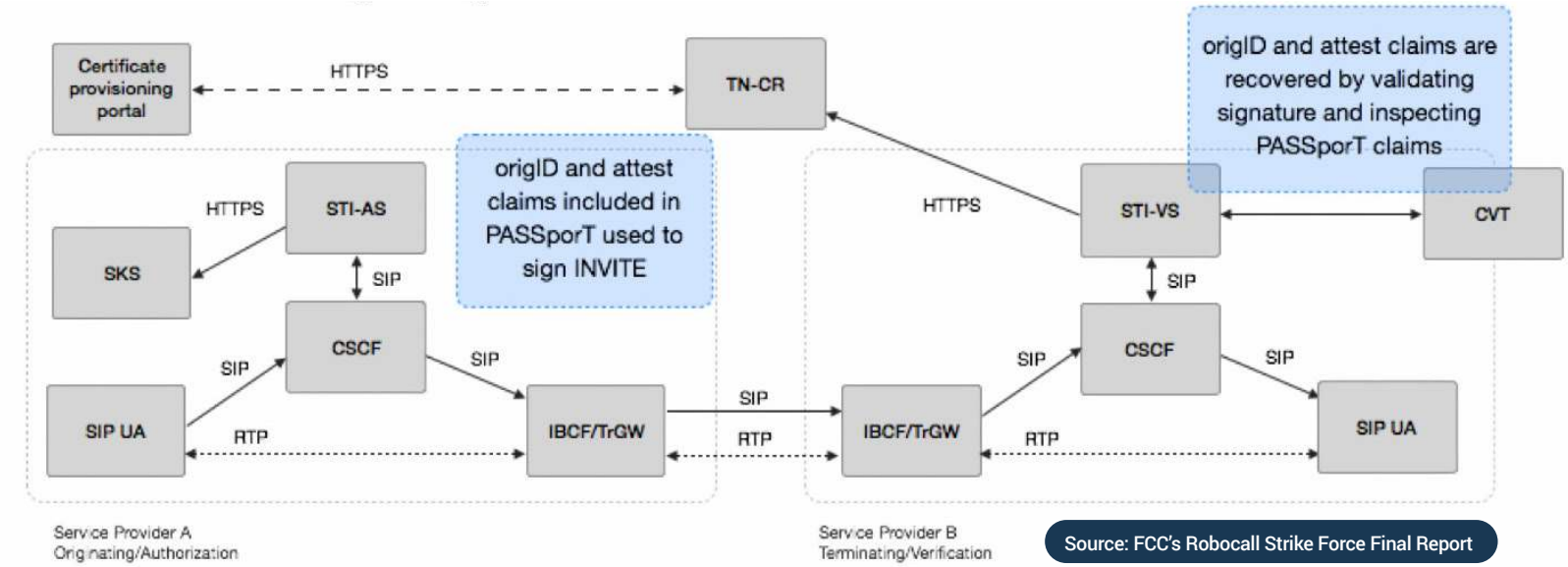
According to the first Robocall Strike Force Report issued by the FCC, the SHAKEN attestation call flow uses the so-called originating identifiers. Let's take a quick look at this process:

1. SHAKEN and the "shaken" PASSporT extension define the ability for the service provider originator to sign the call using claims that represent an attestation ("attest") and unique originating identifier ("origid").

2. The attestation provides the verifier with information on the origination of the call and attestation level the originating provider is giving the calling identity.

3. The originating identifier is useful for both ease of trace back to more granular levels beyond the service provider signing the token and can provide a consistent indicator to analytics for reputation and other metrics.

Attestation and Originating Identifier Call Flow



The system also is expected to enhance the accuracy of companies that provide call-blocking apps for consumers. They already try to block robocalls by looking for calling patterns to identify calls from suspicious numbers, but with reliable caller ID information, this will be far more effective.

SHAKEN is designed to be a flexible solution, with industry-led governance that can adapt to address new scams as they arise. An industry-led governance structure will allow SHAKEN to quickly work toward mitigating new problem calls without cumbersome regulatory measures.

An important point is that the phone network is essentially facing the same problem that email once faced. It was the same situation, when email accounts were littered with spam, to the point that it was feared users might abandon email altogether.

Filters and other anti-spam techniques have brought the email problem under control, even though they have not eliminated email spam. SHAKEN will help us have the same success in mitigating the current problems with the phone network.

STIR/SHAKEN impact for the end consumer

The verification from SHAKEN could be displayed directly to the user or fed into a “call-blocking app” that provides a rating system that essentially identifies calls as good, questionable or likely fraudulent.

The call-blocking app can then act, on behalf of the user to stop unwanted calls from getting through.

In sum, SHAKEN not only gives service providers the tools needed to sign and verify calling numbers, it also makes it possible for consumers to know who is calling, before answering the call.

Consumers eventually are expected to see an as-yet-undetermined signal that will identify calls that have been verified, a feature intended to help guide decisions about whether to pick up. SHAKEN also provides digital signatures for businesses that are allowed to “spoof” telephone numbers.

How Attestation works?

Level A or Full Attestation:

When a STIR/SHAKEN certified carrier knows the individual or the entity making a phone call, and they know the phone number or know that the phone number belongs to that individual or entity, and that they are therefore authorized to use the number. The signing provider:

- *is responsible for the origination of the call onto the IP based service provider voice network.*
- *has a direct authenticated relationship with the customer and can identify the customer.*
- *has established a verified association with the telephone number used for the call.*

Level B or Partial Attestation:

The carrier doesn't necessarily have all the information. So, they might know the caller individual or entity and trust them, but don't recognize the number and cannot attest that they are authorized to use that number for their calls. The signing provider:

- *is responsible for the origination of the call onto its IP based voice network.*
- *has a direct authenticated relationship with the customer and can identify the customer.*
- *has NOT established a verified association with the telephone number being used for the call.*

Level C or Gateway Attestation:

Basically, this is just a transiting call, an international gateway that did not originate on a known network. The carrier doesn't know the customer. They can still say the call passed through the network. The service provider can see the location of the call they received, but they have no authorization for the source, nor can they verify if it is authorized to use the number. The signing provider:

- *is the entry point of the call onto its IP based voice network.*
- *has no relationship with the initiator of the call (e.g., international gateways).*

STIR/SHAKEN assigns an attestation rating of A, B, or C to each call based on key information about the originating caller. These "ratings" assigned by origination service providers (OSP) show how confident they are that the outgoing call is made by the number's owner and that the OSP has validated the caller's permission to use the phone number.

The receiving carrier (also known as the terminating carrier) validates the caller's number and aids in the identification of faked calls by using a decryption key and the attestation rating. Customers can be alerted with a symbol, verification keyword, or alert indicating that the inbound call has been validated, depending on the call handling methodology employed by your service provider.

If the call cannot be confirmed, the carrier may stop it and/or notify the call receiver of a possible scam call. Let's look at the three different levels of STIR/SHAKEN attestation as defined by the FCC:

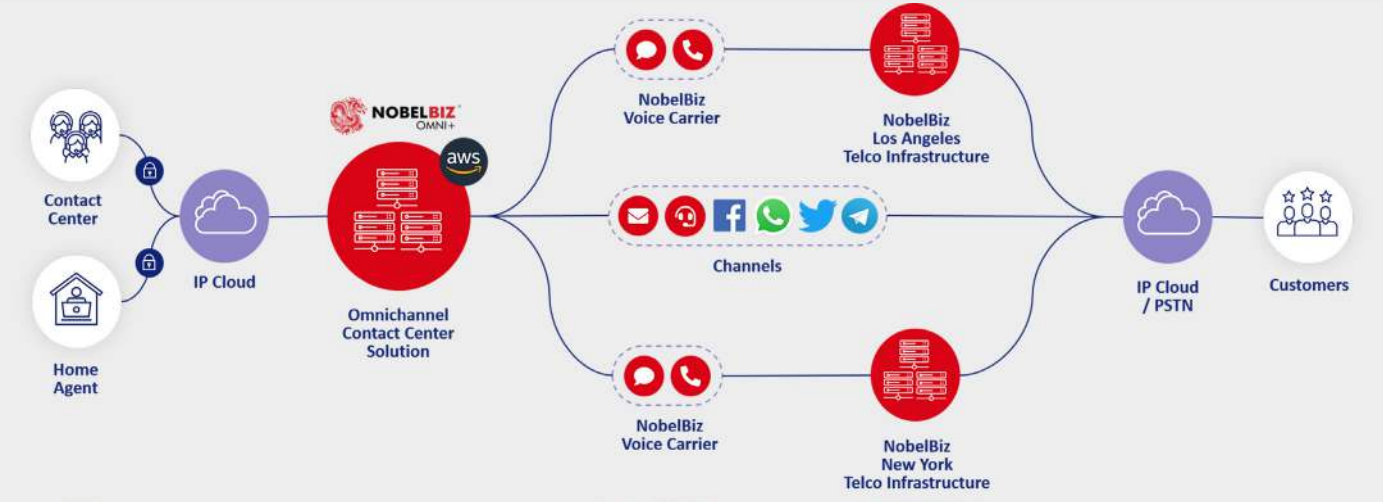
Stir and shake with NobelBiz

NobelBiz supports the initiative to comply with the TRACED act, by offering full STIR/SHAKEN compliance with our telecom network and CCaaS solution, the NobelBiz Voice Carrier Network. We are following the rules defined by the STI-GA (Secure Telephone Identity Governance Authority) and implementing it across our entire network.

Of course, for level A attestation, you, as a call originator, need to meet certain requirements. One thing you need to know is that every carrier has its own validation process.

For any questions you might have or to learn more about the validation process of NobelBiz, give us a call on **800.975.2844** (toll free), or get in touch with one of our experts by going to this **link** and filling the contact form.

Who is NobelBiz?



NobelBiz is a world-class Telecom and CCaaS company with 20 years of experience delivering complete solutions for contact centers across the globe, irrespective of size, industry, or activity.

The **NobelBiz Voice Carrier Network** is the only network built from the ground up to serve contact centers, offering the most versatile selection of smart tools to increase contact rates, mitigate impacts of call labeling and blocking, and provide all-round compliance.

The **NobelBiz OMNI+** cloud contact center software has a unique blend of capabilities: from Omnichannel, Impressive API integrations, and fast implementation, to simple cross-channel campaign setup and remote work.

If you have questions or concerns about the items we outlined, NobelBiz can definitely help you with this. Get in touch with one of our experts.

nobelbiz