

Contact Center Compliance
DNC.com

SHAKEN/STIR Guide

A guide to the call authentication protocol that is a major component of recent robocall regulation efforts

Overview

"Shaken, not stirred."
--James Bond in basically every James Bond novel and movie

With a name that evokes 007's vodka martini preferences, SHAKEN/STIR is an eye-catching bit of telecommunications terminology. But what, exactly, is it?

The most basic explanation is that it is a call authentication framework designed to help telecommunications providers prevent illegal robocalls that make use of caller ID spoofing. This guide will provide a more detailed explanation of what that means, how SHAKEN/STIR came to be, what can be expected for the future, and what the consequences of SHAKEN/STIR are for telemarketers.

Did You Know?
Because each half of the acronym refers to a separate but related protocol, SHAKEN/STIR and STIR/SHAKEN can be used interchangeably.

This content was created for informational purposes only; the information herein is not intended to be legal advice; anyone reading this should not act, or refrain from acting, upon any of the information herein without consulting an attorney.

What is SHAKEN/STIR?

SHAKEN/STIR is a suite of protocols and standards for calls that are intended to combat caller ID spoofing. In order to better explain how it works, we will first define the relevant terms.

Caller ID Spoofing is a technique used by unscrupulous callers whereby they mask their identity by making a call appear as if it is originating from a different phone number than its actual originating station. Oftentimes, robocallers will use caller ID spoofing to appear as if they are calling from the same area code as the recipient of the call.

Fun Fact
In 2006, Paris Hilton was accused of using caller ID spoofing to hack into Lindsay Lohan's voicemail.

STIR stands for **S**ecure **T**elephony **I**dentity **R**evisited. It is a series of call authentication standards to be used for Voice over Internet Protocol (VoIP) calls. It works by adding a digital certificate into the process used to initiate and route VoIP calls—a process known as Session Initiation Protocol (SIP Protocol).

SHAKEN stands for **S**ignature-based **H**andling of **A**sserted information using to**KEN**s. It is a similar set of standards to STIR but it is used for calls to wireless and landline phone numbers rather than VoIP numbers.

The Federal Communications Commission describes SHAKEN/STIR as working such that "calls traveling through interconnected phone networks would have their caller ID 'signed' as legitimate by originating carriers and validated by other carriers before reaching consumers. STIR/SHAKEN digitally validates the handoff of phone calls passing through the complex web of networks, allowing the phone company of the consumer receiving the call to verify that a call is in fact from the number displayed on Caller ID."

History

Caller ID's origins reach back as far as 1968, with the technology becoming widely used by the mid-1990s. Caller ID spoofing followed shortly thereafter, with the first mainstream spoofing service debuting in 2004. The practice became widespread enough that congress passed a law, the Truth in Caller ID Act of 2009, specifically outlawing any caller ID spoofing that is made "with the intent to defraud, cause harm, or wrongfully obtain anything of value"

Did You Know?
The Truth in Caller ID Act's ban on caller ID spoofing allows some exceptions for law enforcement purposes.

In 2016, the FCC formed an industry-led Robocall Strike Force to ask the Alliance for Telecommunications Industry Solutions (ATIS) to suggest remedies for caller ID spoofing. At that point, STIR already existed for VoIP calls and ATIS suggested the creation of SHAKEN for calls to wireless and landline numbers.

By 2018, FCC Chairman Ajit Pai was convinced enough of the promise of SHAKEN/STIR to demand that the telecom industry adopt the protocols. A FCC-led SHAKEN/STIR Robocall Summit followed in 2019, focusing on lessons learned from service providers that had already begun to deploy call authentication technology, and any challenges or technical barriers in the deployment of SHAKEN/STIR by voice providers.

The TRACED Act, a major piece of federal legislation that focuses largely on regulating robocalls, was signed into law at the end of 2019. Among its provisions were directions to the FCC mandating the widespread adoption of SHAKEN/STIR as an industry standard. In April 2020, the FCC adopted an order officially mandating that all phone companies implement STIR/SHAKEN call authentication technology by June 30, 2021.

Consequences for Telemarketers

The practical responsibilities for implementing SHAKEN/STIR lie primarily with the approximately 4,000 telecommunications service providers nationwide. In fact, some major telecom providers such as Verizon and T-Mobile have already begun to implement call authentication frameworks for their wireless customers. However, there are repercussions for callers, as well.

The most important consequence for telemarketers with regards to the eventual widespread adoption of SHAKEN/STIR is ensuring that their legitimate calls are not mistakenly flagged by SHAKEN/STIR. While it's important to note that SHAKEN/STIR is a call authentication framework and does not actually block calls itself, providers can use it to build their own call blocking features.

TRACED Act Safe Harbor

In July 2020, the FCC adopted a new rule as part of its effort to implement the TRACED Act that provides a safe harbor for phone providers who use call authentication frameworks such as SHAKEN/STIR and, as a result, mistakenly block legitimate calls. Thankfully, the order also lays out steps to provide recourse for callers whose calls are undeservedly blocked:

"We require that any voice service provider that blocks calls must designate a single point of contact for callers, as well as other voice service providers, to report blocking errors at no charge to callers or other voice service providers…

Did You Know?

For more than a decade, any call placed from inside the offices of The New York Times appeared to be sent from the phone number 111-111-1111. This practice was instituted to mask the extensions of individual reporters, should any subpoenas of call records be made to try to discover their identities. This practice was discontinued in 2011 in part to comply with legal changes pertaining to caller ID regulations.

"Blocking providers must investigate and resolve these blocking disputes in a reasonable amount of time and at no cost to the caller, so long as the complaint is made in good faith… Blocking providers must also publish contact information clearly and conspicuously on their public-facing websites. We further require that when a caller makes a credible claim of erroneous blocking and the voice service provider determines that the calls should not have been blocked, a voice service provider must promptly cease blocking calls from that number unless circumstances change."

Of course, the FCC is required to balance the sometimes competing interests of different groups, such as providers, callers, and the public at large. And as an agency whose leadership is composed of political appointees, the FCC's priorities can change drastically depending on the ideological bent of the current president and the party that controls congress. As a result, telemarketers need to make every effort to protect themselves from any potential circumstances in which the implementation and regulation of SHAKEN/STIR protocols puts callers at a disadvantage.

Fun Fact
The name for the SHAKEN half (Signature-based Handling of Asserted information using toKENs) of SHAKEN/STIR was specifically (perhaps even torturously) reverse engineered to make the acronym a reference to James Bond and his preference for his martinis to be shaken rather than stirred.

Case Study
In 2019, California Governor Gavin Newsom signed an anti-robocall bill, SB208 Consumer Call Protection Act of 2019, into law. An addition to the Public Utilities Code, the bill required telecommunication service providers to implement SHAKEN/STIR protocols by January 1, 2021. If the providers do not adopt SHAKEN/STIR, they must utilize "alternative technology that provides comparable or superior capability to verify and authenticate caller identification for calls carried over an internet protocol network."

Next Steps

Many cell carriers have already begun to implement SHAKEN/STIR protocols. These systems use a variety of methods to stop unwanted calls, the most prominent of which is the labelling of calls as "scam" or "spam" likely. Carriers use SHAKEN/STIR protocols and spam blocking technology to identify phone numbers which are most likely to be spam. Unfortunately, the technology doesn't only flag bad actors. Many legitimate callers such as health care providers and delivery companies are caught in the crossfire.

What is my spam likely score? How do I find out?
A caller ID reputation monitoring system is essential to keeping track of your spam likely score. Daily monitoring of your outposted phone numbers will ensure your calls are delivered to the intended recipient.

What should I do if my phone number is flagged as spam likely?
There are a number of different actions you can take depending on your circumstances, risk level, and operating environment. The actions you take can include:

1. Rotating to a different phone number with no spam score.
2. Evaluating your dialer settings. Are they too aggressive?
3. Only calling contacts who wish to receive calls from you and have provided **express written consent**.
4. Consider using local touch with a large number of DIDs. In local touch, the phone numbers are scored independently. Additionally, the larger your phone number pool, the less likely a high spam score is to disrupt your other calling activity.