

Guidance for Implementing the STIR-SHAKEN Call Authentication and Robocall Mitigation Mandates in 2021



DECEMBER 2020

The Federal Communications Commission (FCC) has issued rules requiring that certain communications service providers implement the STIR/SHAKEN call authentication framework and other robocall mitigation practices. These rules require significant changes to be made in service provider networks and end user practices by June 2021 in most cases. This guidance is meant to help communications providers determine what their obligations are under the rules.

What is STIR/SHAKEN and how does it work?

STIR/SHAKEN is an industry-developed framework designed to allow communications service providers to distinguish legitimate calls from illegally spoofed calls so that they can take steps to mitigate the illegal calls. STIR/SHAKEN utilizes an encrypted authentication and verification process that establishes a chain of trust between the calling party and the called party. Specifically, the originating carrier (or the earliest carrier in a call chain with authority) is responsible for authenticating calls by “signing” them with an encrypted digital signature and one of three attestations for the callers’ identity: (i) A (or “full”) attestation means the provider can confirm the identity of the caller and the legitimate use of the calling number; (ii) B (or “partial”) attestation means the provider can confirm the identity of the caller but not the telephone number; and (iii) C (or “gateway”) attestations means the provider is the point of entry to the IP network for a call that originated elsewhere, such as a call that originated abroad or on a domestic network that is not STIR/SHAKEN-enabled. When the terminating provider receives a call for delivery to an end user, it is responsible for verifying the call using a verification service and for determining how to treat the call, such as by allowing trusted calls to pass to the called party, showing the called party a warning that the call may be illegitimate, or blocking the call if the provider believes the call is illegal. STIR/SHAKEN only works on Internet protocol (IP) networks.

Who is required to implement STIR/SHAKEN?

The FCC requires “voice service providers” to implement STIR/SHAKEN in the IP portions of their network.

What’s the deadline for implementing STIR/SHAKEN?

June 30, 2021 in most cases, but there are some exemptions discussed below.

Is my company a “voice service” provider?

A “voice service” is broadly defined as any service that is interconnected with the public switched telephone network (PSTN) and that uses numbers from the North American Numbering Plan (NANP). It includes all common carrier voice providers, interconnected Voice over Internet Protocol (VoIP) providers, one-way VoIP services, fax transmissions and services, and over-the-top voice services (e.g., Skype, Google Voice).

Resellers of communications are included within the “voice service provider” definition but do not have control over the way in which their calls are transmitted across the network. Resellers should work with their facilities-based vendor to determine whether outbound calls will be authenticated and how the attestation level of calls will be determined. In addition, resellers should confirm that inbound calls will be verified before being presented for termination.

A communications service provider’s obligations will vary depending upon the role that it serves for particular calls, or even whether it is the provider of voice service on a particular call. Therefore, providers should examine their services closely to determine the extent to which the provider offers voice service on the call.

What does STIR/SHAKEN require voice service providers to do?

The obligations of a voice service provider depend on where the provider is in the call path for a particular call:

- *Originating* providers must: (a) authenticate and verify SIP calls originated and terminated on their networks, and (b) authenticate SIP calls it will exchange with other voice service providers.
- *Intermediate* providers must: (a) pass authentication information to the next provider in the chain unaltered, and (b) authenticate un-signed calls (subject to certain exceptions).
- *Terminating* providers must verify SIP calls they receive from other providers for termination to the end user.

As with the voice services provider definition, an individual service provider could serve different roles for different calls. Thus, a provider may have originating provider obligations for some calls, intermediate provider obligations for others and terminating provider obligations for others. Service providers must be prepared to comply with all of these obligations in their IP networks.

What steps does my company need to take to authenticate and verify calls?

Before a provider can begin authenticating or verifying calls, it must obtain a certificate from the certificate authority designated by the FCC. This first involves obtaining a Service Provider Code (SPC) token from the FCC’s selected governance authority, which indicates that the provider is qualified to receive a certificate. The service provider submits the SPC token to the certificate authority to obtain a certificate. Once the certificate is obtained, the provider or third-party service can begin authenticating and verifying calls. This is a multi-step process with detailed qualification obligations. Please contact us to review the additional requirements before requesting an SPC.

Are there exemptions for implementing STIR/SHAKEN?

There are five exemptions from implementing STIR/SHAKEN:

- *Small Providers* – Providers with 100,000 or fewer subscribers lines have an additional two years, until **June 30, 2023**, to implement STIR/SHAKEN.
- *Unable to Obtain SPC Tokens* – Providers that are unable to obtain the SPC tokens necessary to authenticate calls have an **indefinite exemption** from implementing STIR/SHAKEN until the provider is capable of obtaining a token. However, calls from this service provider may be authenticated by the next carrier in the chain of completion. Such calls are likely to receive a lower attestation level than the originating service provider could provide.

- *Services Subject to Discontinuance* – For services subject to a pending Section 214 discontinuance as of **June 30, 2021**, providers have an additional year, until June 30, 2022, to implement STIR/SHAKEN for the services, unless the service is discontinued before then.
- *Non-IP Portions of Networks* – The non-IP portions of a provider’s network have an **indefinite exemption** from STIR/SHAKEN implementation but are subject to other requirements discussed below.
- *Case-by-Case Exemption* – Providers can petition the FCC’s Wireless Bureau for an exemption or extension for implementing STIR/SHAKEN on a **case-by-case** basis; the formal petition deadline has passed, but the Bureau may still consider new petitions.

What are the requirements for the non-IP portions of my network?

Since STIR/SHAKEN does not work on non-IP networks, the FCC has implemented other requirements for those network portions to mitigate illegal calls. Specifically, by **June 30, 2021**, providers must either (a) upgrade their entire network to IP, or (b) participate in the development of a call authentication standard for non-IP calls (either directly or indirectly through a trade group) *and* implement a robocall mitigation program for the non-IP portions of their networks.

When do I have to implement a robocall mitigation program, and what does that entail?

If a voice service provider qualifies for one of the exemptions noted above, it must implement a robocall mitigation program on the exempted portions of its network. In other words, unless a voice service provider has implemented STIR/SHAKEN across its entire network, a robocall mitigation program is mandatory. We believe it unlikely that any service providers will implement STIR/SHAKEN for all calls by June 30, 2021, so every service provider is likely to have to implement a robocall mitigation program.

There are three required elements of a robocall mitigation program:

1. the provider must take reasonable steps to avoid originating illegal robocall traffic (the FCC recommends the use of reasonable analytics);
2. the provider must commit to respond to requests from the Industry Traceback Group to trace suspect calls for mitigation efforts; and
3. the provider must cooperate in investigating and stopping any illegal robocallers (meaning that the provider must block calls or callers that are believed to be illegal).

How do I demonstrate that my company has implemented STIR/SHAKEN?

All voice service providers must file a certificate with the FCC certifying the implementation status of STIR/SHAKEN on their networks. If STIR/SHAKEN is not fully implemented (again, which we believe will be likely), the provider must describe its robocall mitigation program, including: (i) the type of exemption it received; (ii) the specific steps it has taken to avoid originating illegal robocalls; and (iii) its commitment to fully and timely respond to all traceback requests and to cooperate in investigating and stopping illegal robocallers using its service.

The FCC took a non-prescriptive approach to the robocall mitigation program requirements. A provider’s mitigation program should be tailored to its services and customer base and likely will involve a multi-faceted approach. One-size-fits-all mitigation programs are not likely to satisfy the FCC’s requirements. Please contact us to discuss the creation of a robocall mitigation program suitable for your company.

What happens if I don't implement STIR/SHAKEN or file the required certification?

Beginning 90 days after the date providers are required to submit their STIR/SHAKEN implementation certificate, intermediate and terminating voice service providers are prohibited from accepting calls from any provider that has not filed a certificate. In other words, the calls of a provider that has not filed a certificate will be blocked. Additionally, if the FCC determines that a provider has not implemented STIR/SHAKEN or a robocall mitigation program, as required by the rules, that provider may be subject to forfeitures and other penalties.

Are there special considerations for...?

- *Resellers* – The FCC has specified that the STIR/SHAKEN implementation requirement does not apply to providers that lack control of the network infrastructure necessary to implement the framework, so resellers do not have any implementation obligations themselves. However, because a wholesaler may not have a direct relationship with the resellers' subscribers, the wholesaler may not be positioned to provide higher-level attestations for the subscribers to ensure those calls are trusted. As such, resellers – particularly those with high-volume calling subscribers – may want to utilize contractual mechanisms with their wholesalers so that their subscribers' calls will be signed with the highest attestation level possible.

Further, the robocall mitigation program requirements apply to a reseller regardless of its STIR/SHAKEN obligations. Resellers should develop plans to identify and mitigate unlawful robocalls originating with their customers.

- *Exclusive Wholesalers* – Because wholesalers control the network infrastructure, they are responsible for implementing STIR/SHAKEN or robocall mitigation across their networks and for complying with the certification requirements. Because wholesalers will be responsible for blocking calls that are determined or suspected to be illegal, they may have to block calls from their resale customer subscribers. Additionally, wholesalers may be subject to greater scrutiny if the subscribers of their resale customers generate illegally spoofed calls. Wholesalers should consider using contractual mechanisms with their resale customers to prevent the customers from developing relationships with subscribers who generate illegally spoofed calls and to limit liability when the wholesaler must block the calls of a resale customer's subscribers.
- *Foreign Voice Service Providers* – Although the FCC does not have the authority to mandate that foreign voice service providers implement STIR/SHAKEN, foreign voice service providers are, as a practical matter, obligated to file a robocall mitigation certificate with the FCC that they have implemented a robocall mitigation program in order to avoid blocking of their traffic by downstream providers.
- *International Gateways* – There is no process under the current STIR/SHAKEN framework for international gateway providers to authenticate calls they receive from their foreign provider customers. This is largely because of differences in international standards for call authentication, which are still under development. However, international gateways are permitted to authenticate calls according to industry standards, and thus may be able to obtain relevant information from their customers to satisfy the particular attestation standards established.

Further, although most gateway providers currently are not permitted to obtain an SPC token, the governance authority recently changed its process to permit providers that do not have NANP numbers to obtain SPC tokens upon filing of a robocall mitigation program certification. Providers currently unable to obtain an SPC token should follow implementation of this new policy closely.

Waivers of the FCC requirements

The FCC sought waiver requests for the STIR/SHAKEN implementation requirements by November 20, 2020. Three parties filed waiver requests for certain types of calls, and a fourth party sought a declaratory ruling that STIR/SHAKEN did not apply to a certain call type, or in the alternative, a waiver. The FCC's Wireline Competition Bureau will rule on these requests by March 2021.

Other parties may seek waivers for new problems that arise after November 20th, or for other aspects of the FCC rules. Please check with Kelley Drye if you encounter difficulties in complying with the above requirements and may wish to seek a waiver of FCC rules.

2021 will be a busy year for service providers as the industry works to stand up the STIR/SHAKEN call authentication framework in accordance with the FCC's mandates. Providers should begin immediately to develop implementation strategies suitable for their companies and to establish robocall mitigation programs in compliance with the rules. Please contact us or your regular Kelley Drye contact if you need any assistance.

Kelley Drye Contacts



STEVEN A. AUGUSTINO

Partner

saugustino@kelleydrye.com

(202) 342-8612



CHRIS M. LAUGHLIN

Associate

claughlin@kelleydrye.com

(202) 342-8635

Follow Us

Kelley Drye provides a number of timely and topical communications, including our TCPA Tracker.

Sign up [here](#) to receive Kelley Drye email communications tailored to your interests.



Kelley Drye's Full Spectrum Podcast

www.kelleydryefullspectrum.com



COMMLAW MONITOR BLOG

www.commlawmonitor.com



Twitter

@KelleyDryeComm

www.twitter.com/KelleyDryeComm