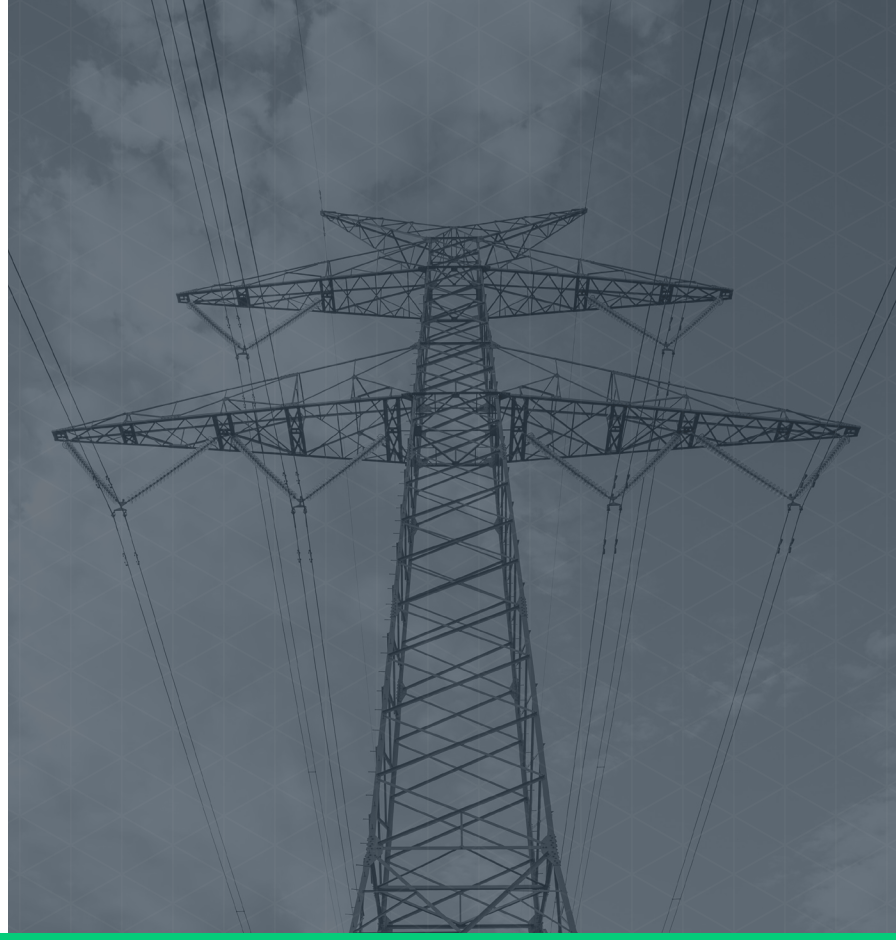
FCC Updates and Best Practices on STIR/SHAKEN.

neustar®
A TransUnion® Company

The Federal Communications Commission (FCC) has taken a series of measures to help put an end to illegal caller ID spoofing. Key to their broader efforts has been their work to promote the implementation of the STIR/SHAKEN caller ID authentication framework.

STIR/SHAKEN promises to help protect consumers from malicious spoofing by enabling voice service providers to verify that the caller ID information transmitted with a call matches the caller's phone number.



What's STIR/SHAKEN?

The TRACED Act mandated that all Communications Service Providers (CSPs) implement STIR/SHAKEN as the caller ID authentication framework in the Internet Protocol (IP) portion of their networks by June 30, 2021.

STIR Secure Telephony Identity Revisited

SHAKEN Secure Handling of Asserted Information Using Tokens

The FCC and STIR/SHAKEN

DEC 2019

Congress passes Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act.

Directs FCC to take numerous steps to promote and require STIR/SHAKEN implementation.

MAR 2020

FCC mandates that service providers implement STIR/SHAKEN call authentication technology in the Internet protocol (IP) portions of their phone networks by June 30, 2021.

OCT 2020

FCC issues Second Report and Order. Recognizing that many smaller carriers are critical to the cause and may require more time to address certain challenges, the FCC made specific allowances and required robocall mitigation solutions as an interim measure.

DEC 2020

FCC Fourth Report and Order. Expands safe harbor based upon reasonable analytics to cover network-based blocking; requires CSPs work with FCC and law enforcement on tracebacks; and more.

TCPA Report and Order. Limits the number of non-telemarketing calls made to residential phones for the first time.

APR 2021

FCC public notice mandated that CSPs file certifications about what they're doing to stop illegal robocalls from originating on their networks in the new Robocall Mitigation Database by June 30, 2021. Even carriers that were granted an extension to STIR/SHAKEN call authentication implementation deadline must provide detailed information about measures they are taking to ensure they are not the source of illegal robocalls.

JUNE 2021

Deadline for CSPs to implement STIR/SHAKEN unless they received an extension.

SEPT 2021

Beginning September 28, 2021

Intermediate and terminating CSPs have to block calls from service providers that are not listed in the database.
The result? Some subscribers will be unable to complete calls when the recipient is not on the same name network.

JUNE 2022

Small- to mid-sized non-facilities-based carriers that received extensions must implement STIR/SHAKEN in the IP portions of their networks.

FCC's Wireline Competition Bureau calls upon North American Numbering Council (NANC) via its Call Authentication Trust Anchor (CATA) Working Group (WG) to recommend Best Practices for the Implementation of Call Authentication Frameworks.

STIR/SHAKEN and Robocall Mitigation: A Perfect Pair

To be successful, STIR/SHAKEN must work hand-in-hand with robocall mitigation solutions. The FCC is also requiring that carriers implement such solutions not only while working to implement STIR/SHAKEN, but also on an ongoing basis.

ROBOCALL MITIGATION

Helps protect your subscribers from robocalls reaching your network and stops bad actors from originating from your network.

STIR/SHAKEN

Helps ensure that calls originated from your network are trusted and that calls to your subscribers are authenticated.

The FCC is Laser-Focused on STIR/SHAKEN

After manding that all Communications Service Providers (CSPs) implement STIR/SHAKEN in the IP portion of their networks by June 2021, the FCC followed up with a **Second Report and Order** that offered extensions to many small carriers, and required robocall mitigation solutions be implemented by all CSPs as an interim measure.

Then, to guide service providers through the process, they engaged the North American Numbering Council (NANC) via its Call Authentication Trust Anchor (CATA) Working Group (WG) to recommend **Best Practices for the Implementation of Call Authentication Frameworks**.

Most recently, in their **April 2021 public notice**, the FCC announced the launch of the FCC Robocall Mitigation Database, mandating that CSPs file certifications about what they're doing to stop illegal robocalls from originating on their networks in the new database by June 30, 2021. Even carriers that were granted an extension to the STIR/SHAKEN deadline had to provide detailed information about measures they are taking to ensure they are not the source of illegal robocalls.

STIR/SHAKEN REQUIREMENTS

Under the current Governance Authority rules, a CSP must meet certain requirements to receive a certificate to participate in the STIR/SHAKEN ecosystem:

- A current FCC Form 499A on file with the Commission
- An Operating Company Number (OCN)
- Direct access to telephone numbers from the North American Numbering Plan Administrator (NANPA) and the National Pooling Administrator

Robocall Mitigation Solutions: A Good Interim and Long-Term Measure

By requiring that robocall mitigation programs be implemented by everyone – those who are and those who are not currently implementing STIR/SHAKEN – the FCC is underscoring the need for CSPs to take immediate action to demonstrate their commitment to combatting robocalls.

In addition to striving to implement STIR/SHAKEN, which ensures that calls from your network are authenticated and trusted, CSPs must have a robust program in place to prevent illegal calls from originating from their network. This is different from traditional robocall analytics programs that identify suspicious inbound calls. This is not a temporary stop-gap measure, but an ongoing measure to reduce robocalls.

FCC Second Report and Order (October 2020)

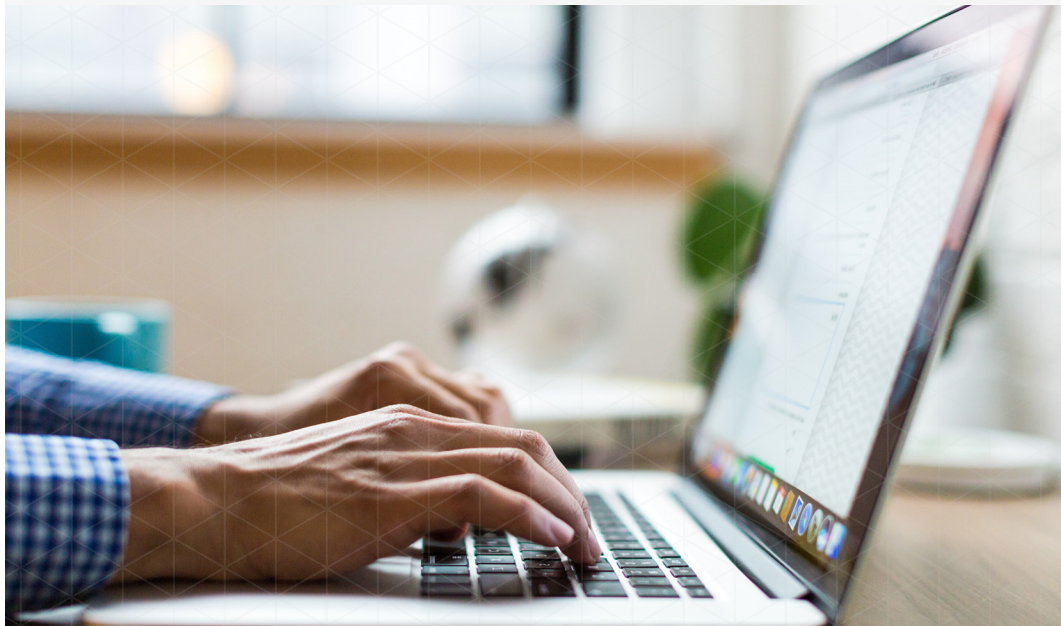
Extensions Granted to Carriers Facing Hardship

Carriers that can demonstrate why implementing STIR/SHAKEN would cause a significant burden are eligible for an extension. FCC granted:

- A 2-year extension to CSPs with less than 100,000 subscriber lines
- A 1-year extension for services scheduled for Section 214 discontinuance
- Extensions as necessary for CSPs that cannot obtain a Governance Authority's token and non-IP networks that cannot support STIR/SHAKEN

CSPs Claiming Extension Must Implement Robocall Mitigation on Networks

- All carriers that were granted an extension were required to implement a robocall mitigation program that reduces robocalls from originating from their network by June 30, 2021 – that's an important stop-gap measure until it's possible to implement STIR/SHAKEN.



Expanded Definition of CSPs to Include Over-the-Top (OTT) Carriers

To enable as many organizations as possible to participate in STIR/SHAKEN ecosystem while keeping bad actors out, OTT carriers are now subject to the rules of the TRACED Act.

However, there are many OTT providers that do not qualify to receive a token based upon the current criteria. A carrier must:

- Have a 499A on file with the FCC
- Have an Operating Company Number (OCN)
- Obtain direct access to telephone numbers (TNs) – the most common reason VOIP providers do not qualify for a token.

FCC TCPA Report and Order (December 2020)

In its Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, published on December 29, 2020, the FCC limits the number of non-telemarketing calls made to residential phones for the first time. Taking steps to implement section 8 of the TRACED Act, the FCC:

- Codified exemptions for calls to wireless numbers into our rules to clarify exemptions for callers and consumers
- Amended the TCPA exemptions for calls made to residential telephone lines to ensure each satisfies the requirement to identify who can call, who can be called, and any call limits

Those exemptions are for:

- Non-commercial calls to a residence
- Commercial calls to a residence that do not include an advertisement or constitute telemarketing
- Tax-exempt nonprofit organization calls to a residence
- HIPAA-related calls to a residence

FCC Fourth Report and Order (December 2020)

Put into effect on December 29, 2020, the goal of the FCC's fourth report and order was to require service providers to take specific actions to better police their networks against call spoofing, including expanding safe harbors, necessitating greater transparency, and more. Details include:

- Expands safe harbor based upon reasonable analytics to cover network-based blocking if the network-based blocking incorporates caller ID authentication information
- Must target only calls highly likely to be illegal, not simply unwanted
- Must manage blocking with human oversight and network monitoring to ensure the blocking works as intended
- Voice service providers must work with the FCC, civil and criminal law enforcement, and the Traceback Consortium on trace back requests. Requires voice service providers to prevent *new and renewing customers* from using their network to originate illegal calls.

FCC Public Notice (April 2021)

All Service Providers Must File a Certification in FCC Database

The FCC has created a **Robocall Mitigation Database** that tracks the compliance status of all carriers robocall mitigation efforts (STIR/SHAKEN, robocall mitigation, exemptions, etc.) as outlined below:

- Carriers that use NANP telephone numbers (including foreign entities) are required to file a certification in the FCC database to demonstrate that traffic is either signed with STIR/SHAKEN or subject to a robocall mitigation program, or have an exemption

Impact of the FCC Database

- The policy is extended to any foreign CSP that uses NANP numbers that pertain to the United States to send voice traffic to subscribers in the U.S.
- To appear in this database, CSPs must also agree to cooperate with the FCC, law enforcement, and the ITG to investigate and stop any illegal robocalls that it learns are using its service to originate calls
- Intermediate providers and terminating CSPs will be prohibited from accepting voice traffic directly from any CSP not in this database
- Carriers are **required to block calls** from carriers that did not have a certification on file by September 28, 2021

STIR/SHAKEN Small Provider Report and Order (December 2021)

Through its work with Industry Traceback Group (ITG), the Federal Communications Commission (FCC) has identified that small carriers are a major source of robocalls. As a result, on December 10, 2021, the FCC adopted an order that accelerates the deadline for small carriers to implement STIR/SHAKEN by a full year.

The new deadline was June 30, 2022 (previously June 30, 2023).

The revised deadline applies to certain small carriers that are not facilities-based. They are required to implement STIR/SHAKEN in the IP portions of their networks.

If the FCC notifies a carrier that they are suspected of originating robocalls, the carrier will have 90 days to implement STIR/SHAKEN.

The new deadline was June 30, 2022 (previously June 30, 2023).

Putting It All Into Practice: CATA Working Group Best Practices

As part of the TRACED Act, Congress directed the FCC to issue best practices to CSPs. On the next page are the top recommendations developed by the American Numbering Council (NANC) via its Call Authentication Trust Anchor (CATA) Working Group (WG) in their Best Practices for the Implementation of Call Authentication Frameworks.

Seven Recommendations for Service Providers

1. **Subscriber Vetting:** vet the identity of retail and wholesale subscribers, along with approving an application for service; provisioning of network connectivity; entering into a contract agreement; or granting the right-to-use telephone number resources.

2. **TN Validation for OSPs:** confirm the end-user or customer's right-to-use a TN.

3. **A-Level Attestation for OSPs:** authenticate calls with attestation level A only when confident attest the end-user originating the call is authorized to use the TN-based caller identity associated with the calling line or account.

4. **B- and C-Level Attestation for OSPs:** authenticate calls with attestation levels B or C for calls where TN Validation has not been performed on the originating TN.

5. **Third-Party Validation Services for OSPs:** use a third-party validation service when they can't/choose not to do it themselves.

6. **International:** when selling services to international call originators using North American Numbering Plan (NANP) numbers, develop processes to validate that the calling party is authorized to use the TN or caller identity. Domestic gateway providers may wish to explore commercial arrangements with international providers that include terms and conditions that would give the domestic gateway provider the tools, information, and confidence to trust the validity of the calling identity.

7. **Ongoing Robocall Mitigation:** whether IP- or non-IP-based, have ongoing robocall mitigation programs in addition to implementing call authentication protocols, which may include ongoing monitoring of subscriber traffic patterns to identify behaviors that are consistent with illegal robocalling. After investigation, service providers can then take appropriate action to address such behaviors.

Three Reasons to Start STIR/SHAKEN Implementation Now!

Although the extensions granted in the FCC's Second Report and Order are likely to apply to many small carriers, there are still many compelling reasons for carriers of every size to pursue STIR/SHAKEN now.

REASON 1

Help Ensure Your Subscribers' Calls Are Answered

As many large carriers have already implemented STIR/SHAKEN (covering nearly 70% of U.S. telephone numbers), service providers that have not will likely see their calls negatively impacted. When calls from OSPs that have not implemented STIR/SHAKEN are received by TSPs, the TSP may mark the call as "SPAM Likely" or the recipient may not trust the call as it does not have a verification indicator – putting your subscriber's calls in jeopardy.

REASON 2

Help Protect Your Subscribers from Illegal Spoof Robocalls

Carriers that don't implement STIR/SHAKEN won't receive STIR/SHAKEN indicators that the calls made to their subscribers are authentic – you cannot detect when a call has been spoofed.

REASON 3

Retain Your Voice Revenue

Nearly 60% of small carrier's revenue comes from voice services which means it's critical that the phone remains a trusted channel.

Neustar, a TransUnion company's, **Robocall Mitigation solution** works alongside STIR/SHAKEN call authentication to identify unauthorized and suspicious use of phone numbers and to detect trends and anomalies in calling patterns. It helps mitigate robocalls originating from, or terminating on, their network.

Authoritative Data

Access Neustar's broad range of proven data to identify, flag and classify risk of a phone number and calculate a fraud score

Real Time Alerts

Receive notifications about telephone numbers originating suspected illegal robocalls, including from unassigned, inactive, and do-not-originate TNs

Advanced Fraud Detection

Leverage behavior analysis and tracking of abnormal and unexpected calling patterns to detect high volume robocalling, spoofing, and suspicious call activity

Global Block and Warn

Define policies to block calls across the network or display notifications (e.g., "Robo-Caller") to help protect subscribers and improve the call experience

Learn More.

Neustar, a TransUnion company, is a pioneer in call authentication as the co-author of STIR standards and early contributor to the SHAKEN framework, and we play an ongoing leadership role in defining industry standards with ATIS, IETF, and CRTC. We provide the industry's reference implementation of STIR/SHAKEN as the exclusive operator of the ATIS Robocalling Testbed, where real world STIR/SHAKEN implementations are being tested for interoperability, and Neustar leads the industry in commercial call authentication deployments. Visit our **STIR/SHAKEN Resource Hub** to learn about insights, resources, and solutions. And learn how you can implement robocall mitigation solutions today.

Contact us at 1-855-898-0036.

This document is not intended to be used as legal guidance. Please consult your legal resources for help interpreting the laws and regulations.

EB-CSP-269483 07.20.2022

neustar®
A TransUnion® Company