



Compliance

[Tax and FCC Considerations](#)

[HIPAA Compliance](#)

STIR/SHAKEN Compliance

[Service Provider Guide to CoreDial's CPNI Policy](#)

[Introduction to Federal and State Indirect Taxes for Telecommunications Resellers](#)

[DNO \(Do Not Originate\) FCC Order](#)

Suggested articles

[Robocall Mitigation Database Filing Requirements](#)

[Why is my number showing as SPAM?](#)

[DNO \(Do Not Originate\) FCC Order](#)

[Glossary of Terms](#)

[LNP FAQs](#)

STIR/SHAKEN Compliance

STIR/SHAKEN is an industry-standard Caller ID authentication technology that enables subscribers to trust that callers are who they say they are, reducing the effectiveness of fraudulently spoofed calls. This authentication technology is critical in protecting Americans from scams using spoofed robocalls because it erodes the ability of callers to illegally spoof a caller ID, which is a common scam tactic used to trick Americans into answering their phones when they shouldn't.

The STIR/SHAKEN solution also allows consumers and law enforcement alike to more readily identify the source of illegal robocalls and reduce their frequency and impact.

Partner Brief - Must Read

CoreDial submitted its filing in the Robocall Mitigation Database, per FCC requirements.

Handling for CoreDial DIDs

- For calls originating from the CoreDial network, CoreDial will make attestation level A for calls whose Caller ID is a phone number purchased directly from CoreDial.
- Sip trunks that can set passthru/custom caller id/forwarded calls = B

Handling for BYOC

BYOC partners should work with their underlying carriers for guidance for their STIR/SHAKEN call handling.

CoreDial Robocall Mitigation Plan

As part of STIR/SHAKEN enforcement, on April 20, 2021, the FCC began requiring all providers to certify in the Robocall Mitigation Database that they have fully implemented STIR/SHAKEN or have instituted a robocall mitigation program to ensure that they are not originating illegal robocalls. Our CoreDial policies are aligned with this FCC regulation, as detailed below.

The handling policies submitted under CoreDial's robocall mitigation program are as follows:

- Software introduced to monitor outbound voice traffic in real-time to prevent the origination of illegal robocalls.
- The software provides detailed reporting identifying suspected illegal robocalls and alerts CoreDial if CoreDial originates any calls where the calling number is:
 - Invalid
 - Unallocated
- CoreDial will immediately investigate any identified calls to determine if the caller was attempting to originate unlawful robocalls. If we determine that the caller was attempting to originate unlawful robocalls, then we either warn them to stop or terminate their service as appropriate.

For Partners who utilize CoreDial Origination and Termination Services

Invalid or Offending Origination Calls:

- In the future, calls will not be allowed to egress our Network, with an exception of 911 Calls.

STIR/SHAKEN FAQs

Will CoreDial allow a number to be spoofed temporarily for Porting In purposes?

Yes, so long as it is compliant with our robocall mitigation program.

When will CoreDial provide attestation indicators on inbound calls?

This is currently being reviewed with our vendors and equipment manufacturers for best practices. At this time we do not have an expected release date.

How did we get to where we are today with STIR/SHAKEN?

It all points back to Caller ID spoofing by robocallers to try to dupe or defraud consumers. Most of the traffic predominantly originated on VoIP provider networks all around the world, in some cases with the audacity to spoof government telephone numbers at times. This pattern created a major initiative to stop robocalls in Canada and the US which eventually evolved into a concept called STIR/SHAKEN which is now being enforced by the CRTC and FCC.

What is STIR/SHAKEN expected to do?

STIR/SHAKEN is designed to create a measure of trust in the displayed caller name and number by authenticating the calling number. STIR/SHAKEN is NOT going to eliminate spam calls immediately, the most immediate benefit to the FCC/CRTC and Law Enforcement is having the ability to trace calls back to their Origin.

Why is it called STIR/SHAKEN?

STIR (*Secure Telephone Identity Revisited*) has been defined as a series of RFC standards used to create a digital signature key for a call by a working group within the IETF, an internet standards body. The signed call includes information about the calling party and allows for verification of the signature by the terminating provider.

SHAKEN (*Signature-based Handling of Asserted Information Using toKENs*) is the standard for handling how STIR is to be deployed by service providers within their networks.

In the STIR/ SHAKEN framework, digital signatures also referred to as tokens shall be issued to carriers or others who own or are assigned dedicated telephone numbers. A trust factor or Attestation Level will be sent by the sending carriers in the call stream for the receiving carriers to determine how they want to handle the call. The levels are as follows:

- **“Full” Attestation A** - The provider knows the customer, they know the customer has a right to use the originating number, and they know that the call originated on their network.

- **“Partial” Attestation B** - The provider knows the customer but the customer may be using another provider's number. The call is legitimate but the provider can't fully attest because of missing info (No Token in the SIP stream).
- **“Gateway” Attestation C** - The provider can't verify the customer or phone number and has no way of knowing whether the call is legitimate, however, they attest to the call to mark that it originated on their network.

Who is required to participate in STIR/SHAKEN?

All voice providers operating in N. America. The magnitude of the implementation with all voice providers is enormous, as there are 15,000+ CLEC's in the United States operating various switching platforms for call processing via SIP and or traditional SS7 signaling. As of today, the major carriers, T-Mobile, Verizon, and ATT have begun to sign many of their calls between each other with tokens. We expect full implementation across all service providers to take quite a bit of time.