Restoring Trust in Calls with STIR/SHAKEN

The rise in unwanted calls afflicts almost everyone with a phone in the U.S. today. And even more distressing are the calls where fraudsters hide their identity, by spoofing or changing the caller ID, to try to dupe or defraud consumers. To protect themselves, most consumers do not answer unless they are certain who is calling. For legitimate businesses, the impact is that they are often unable to contact customers by phone to relay important or sensitive information.

The top consumer protection priority of the Federal Communications Commission (FCC) is stopping illegal robocalls, and they have a number of actions underway. To specifically address caller ID spoofing, the FCC has directed carriers to implement robust call authentication by adopting STIR/SHAKEN standards targeting the end of 2019. What does this mean for carriers?

STIR and SHAKEN are the most viable way to provide a measure of trust in the displayed caller name and number by authenticating the calling number. STIR (Secure Telephony Identity Revisited) is a set of technical standards developed by the Internet Engineering Task Force (IETF) to certify the identity of originating calls and SHAKEN (Signature-based Handling of Asserted information using toKENs) is a framework developed by the Alliance of Telecommunications Industry Solutions (ATIS) that focuses on the implementation of STIR within IP-based service provider networks.

In a recent webinar hosted by Neustar, Restore Trust in Phone Calls: Meeting the FCC Call to Action with STIR/SHAKEN, we shared important next steps in implementing call authentication. Here are some of the questions from our webinar attendees on their concerns and challenges in implementing STIR/SHAKEN, with answers provided by our team of experts. Neustar is a pioneer in call authentication, co-author of the STIR/SHAKEN standards and market leader and neutral trusted provider of caller ID services in the U.S.

Q: Is there a difference between robocalls and spoofed calls?
A: Robocalls are a programmatic origination of calls, usually done in high volume, which can deliver either a recorded message or a live person on the line. Legal robocalls are used for quickly getting out important messages such as for school closures or weather alerts. Call spoofing is when a call originator changes the calling number, for the purpose of hiding or controlling which calling number is shown on the call display. An example of a legal use of spoofing is to present a main callback number for call centers or customer support, or to keep a calling number private such as when a doctor contacts a patient from their private phone. However, many parties illegitimately spoof numbers today when they wish to avoid detection or trick users into picking up unwanted calls. Currently, the illegal calls causing a big problem in the U.S. are often a combination of automated dialing with spoofing for the intent to defraud consumers.
Q: How did call spoofing get to be such a big problem?
A: Initially, the telephone network was a closed network for internationally licensed carriers who had authorized access to the underlying signaling network, using the SS7 protocols. The Session Initiation Protocol (SIP) was designed to place Voice over IP (VoIP) telephone calls over the Internet, and enabled a feature similar to email where a ‘From’ header field could be set by the call originator. However, there were some unanticipated consequences when the SS7 network and the Internet were connected by gateways which ultimately compromised security: there was no mechanism to verify the originating telephone number at a gateway. Gateways generally accepted the calling number provided on the Internet side and propagated it into the public switched telephone network (PSTN) and thus the caller ID ecosystem. With so many VoIP networks today interconnected with the PSTN, it is now cheap and easy to spoof caller ID and deliver virtually untraceable phone calls.

Q: Why is STIR / SHAKEN the best way to address caller ID spoofing?
A: STIR/SHAKEN brings together the security that keeps e-commerce safe on the Internet with telephone security that provides a way of knowing whether a caller has the right to use a given telephone number. The most proven way to attest to an identity on the Internet is with a digital certificate. In the STIR/SHAKEN framework, digital certificates are first issued to carriers, or others who own or are assigned dedicated telephone numbers. The private key associated with a digital certificate is then used to sign a VoIP call, thereby indicating that the calling party number has been properly attested. Calling numbers that cannot be verified by terminating carriers are ones that may have been spoofed.

Q: How can a carrier implement STIR/SHAKEN if they only have traditional TDM trunks, and not SIP trunks?
A: There are a variety of ways that carriers with traditional TDM trunks can implement STIR/SHAKEN:

- A STIR/SHAKEN-aware gateway can be put in front of legacy infrastructure. This will enable calls to show up as being valid signed calls at their destination.
- If there are endpoints or intermediaries in the legacy TDM infrastructure that can access the Internet, there can be an implementation of an out-of-band infrastructure for STIR/SHAKEN.
- An upstream carrier with a gateway can potentially sign calls on behalf of the carrier with traditional TDM trunks.

Q: 98% of complaints we get are about telemarketing calls from local numbers. In most of these cases, the origination party owns the local calling numbers. Therefore, the numbers would be successfully authenticated. How does STIR/SHAKEN address this issue?
A: This is also referred to as ‘neighbor spoofing’ and is used to make it look like a call is from a local number. While most neighbor spoofing results from caller ID spoofing, some more sophisticated illegal robocallers do acquire legitimate numbers in local NPA/NXXs for this purpose. What STIR/SHAKEN adds in this case is a new layer of accountability. Currently, there is no effective way to trace back who the calling entity for these calls is. With STIR/SHAKEN, if a call is ‘neighbor spoofed’, it can be more quickly traced to the carrier signing the call and further isolated within that carrier’s network. We anticipate that more punitive legal and policy measures are likely to be introduced for people who issue illegal robocalls like these using ‘neighbor spoofing’.
**Q:** Why should we flag calls rather than block them?

**A:** Businesses and industry associations, such as PACE (Professional Association for Customer Engagement), have spoken out on issues from blocking calls and the impact of business to consumer calls not going through or being mistakenly marked as spam. An example often shared is in regards to pharmacies and how their calls were being marked as spam by some solutions when they were just trying to send out prescription information. Consumers and businesses do not want important calls like these being blocked.

In Neustar’s work with a large number of enterprises, we discovered that almost all have experienced some of their calls being wrongly blocked or marked as spam. This can be partly attributed to call analytics programs that just look at volume metrics and crowdsourcing to determine whether a call should be marked as spam or blocked. And with anyone having the ability to mark a telephone number as being ‘bad’ from their mobile device, not all data sources are authoritative. We believe it is best practice to inform the consumer about who is calling and empower them to make the decision about whether they want to answer that call or not. Consumers will have the tools to set their own policies around how much receptive they are to communications with the reliable information that STIR/SHAKEN provides.

**Q:** How are other countries participating in STIR/SHAKEN?

**A:** In the U.S. there is an industry process with the Call Authentication Trust Anchor Working Group (CATA), with endorsement by the FCC, to define the trust anchor for STIR/SHAKEN. For countries to participate in STIR/SHAKEN, they will most likely need to go through a similar regulatory process. In Canada, the CRTC has recommended that STIR/SHAKEN be put into effect in 2019 and are now working through a similar process to define the trust anchor. A number of regulators in Europe, including Ofcom, are tracking the progress of STIR/SHAKEN adoption in the U.S. and are at various stages of developing initiatives in their own countries.

**Q:** How can enterprises use STIR / SHAKEN and call authentication?

**A:** SHAKEN is a carrier-centric framework that sets out a standard way to implement STIR on the Internet Protocol-based Network-to-Network Interface (IP-NNI), the interface that carriers establish for exchanging VoIP traffic. Enterprises that have their own VoIP infrastructure are expected, at some point, to have the option to set up call authentication through a new STIR/SHAKEN delegation feature. With this new feature, carriers can delegate authority for telephone numbers assigned to enterprises so an enterprise can effectively and more equally participate in the STIR/SHAKEN ecosystem.

**Q:** I received a spam call for a phone number identified as one used in England. Will these standards work with international originated callers?

**A:** Any originating call from another country has an ingress or entry point into the U.S. network, and the carrier that brings the call into the U.S. has the ability to sign it. SHAKEN has a provision for signing calls like this as the ‘gateway level of attestation’. This information can be useful as an input to call analytics programs used to help warn/advise consumers about answering a call.