Frequently Asked Questions (FAQ)

Q. **What does SHAKEN stand for?**

A. SHAKEN stands for Signature-based Handling of Asserted information using toKENs. It is a specification designed specifically to mitigate unwanted robocalls by reducing the impact of caller ID spoofing. Unwanted calls are the number one source of recent complaints to the FCC, and caller ID spoofing increases the harm from these unwanted calls.

Q. **Who developed SHAKEN?**

A. It was developed by the ATIS-SIP Forum IP-NNI Task Force. IP-NNI stands for “Internet Protocol - Network to Network Interface.” SIP stands for Session Initiation Protocol. SHAKEN is based on the STIR (Secure Telephone Identity Revisited) protocol developed by the IETF (Internet Engineering Task Force) which is why it is typically referred to as STIR/SHAKEN.

Q. **How does SHAKEN work?**

A. The verification system is designed to correct an unforeseen consequence of technology evolution that began to emerge during the late 1990’s. That’s when the telecommunications industry launched a technology capable of transmitting telephone voice calls via a broadband Internet connection instead of a regular phone line and dramatically reduced the cost of making phone calls. Robocalls use VoIP because it's inexpensive. It also enables some users to

enter anything they want as the source of the call. That identification, true or false, automatically is conveyed to the called consumer.

STIR is a call-certifying protocol developed by the Internet Engineering Task Force or “IETF.” The SHAKEN framework complements the STIR protocol by providing guidance for service providers to implement STIR in carrier networks. STIR/SHAKEN allows the originating carrier to generate a digital signature that securely signals the caller's right to use a phone number to the terminating carrier. STIR/SHAKEN will offer a practical mechanism to provide verified information about the calling party as well as the origin of the call — what is known as “attestation.”

When you make a call, your phone carrier will use your identifying number to create a digital signature, or token, that will accompany the call as it is being completed. At the other end, the system verifies that nothing was tampered with and ensures that the call came from someone who has a legitimate right to use that number. Phone calls typically pass through multiple carriers as they travel from caller to recipient. Say, for instance someone who uses AT&T calls someone who uses Verizon, T-Mobile or another carrier. A caller’s phone provider has always known something about the origin of the call and whether the caller ID is authentic. But until now, that provider had no secure way of passing the information along.

SHAKEN provides a reliable way to do that, using encrypted digital signatures for each call that lets the user know that the caller ID information is accurate. The verification from SHAKEN can be displayed directly to the user or fed into a “call-blocking app” that provides a rating system that essentially identifies calls as good, questionable or likely fraudulent. The call-blocking app can take action, on behalf of the user, to stop unwanted calls from getting through. In sum, SHAKEN not only gives service providers the tools needed to sign and verify calling numbers, it also makes it possible

for consumers to know, before answering, that the calls they receive are from legitimate parties.

However, SHAKEN is not a silver bullet solution to the problem of unwanted calls.

It won't block any phone calls – including robocalls. The network is designed to get calls through. Consumers eventually are expected to see an as-yet-undetermined signal that will identify calls that have been verified, a feature intended to help guide decisions about whether to pick up. The system also is expected to enhance the accuracy of companies that provide call-blocking apps for consumers. They already try to block robocalls by looking for calling patterns to identify calls from suspicious numbers, but with reliable caller ID information, this will be far more effective.

SHAKEN is designed to be a flexible solution, with industry-led governance that can adapt to address new scams as they arise. An industry-led governance structure will allow SHAKEN to work toward mitigating problem calls without cumbersome regulatory measures.

An important point is that the phone network is essentially facing the same problem that email once faced. Many of us remember a time when our email account was littered with spam, to the point that where we feared users might abandon email altogether. Filters and other anti-spam techniques have brought the email problem under control, even though they have not eliminated email spam. SHAKEN will help us have the same success in mitigating the current problems with the phone network.

Q. **When will SHAKEN be up and running? When will I stop getting these calls?**

A. Fraud calls won't vanish overnight. But the phone system has fewer points of entry and fewer paths to monitor than the wide-open spaces of the Internet. Knowing when incoming Caller ID correctly identifies the caller, and that a malicious party can be more easily identified, could finally cut off the scammers. We should start seeing SHAKEN's impact within the next few years.

Seeing the value in the SHAKEN solution, in November 2018, FCC Chairman Ajit Pai said in a statement that he demanded that the phone industry adopt a robust call authentication system to combat illegal caller ID spoofing and launch that system no later than next year—2019.

Q. **When was the RFP Issued?**

A. The STI-GA issued a request for proposals for a Secure Telephone Identity Policy Administrator or "STI-PA," to apply and enforce the STIR and SHAKEN rules. Responses were received on February 4. The selection process is expected to conclude in or about May 2019. Once the STI-PA is named, carriers will work toward meeting the end of the year goal to set SHAKEN into action in the network.

Q. **What will the user see when SHAKEN is deployed? Will they see a "green checkmark" or "red X"? If they don't see anything, how will they regain confidence in the phone network?**

A. It is currently up to individual service providers to decide how they would like to communicate the information SHAKEN provides to their customers. The IP-NNI Task Force is debating the optimum

strategy for what to display to the end user, based on SHAKEN verification. But independent of what is displayed to the end user, SHAKEN will enhance the effectiveness of call-blocking apps and FTC enforcement actions, both of which will reduce the negative impact of unwanted calls. Over time, these will help consumers to regain confidence in the phone network.

Q. **How much will it cost to solve this problem?**

A. Individual service providers bear the costs of setting SHAKEN into action in the network. ATIS cannot comment on this

Q. **Who is making these calls? Where do they originate from?**

A. The bulk of the unwanted robocalls calls are from international sources, although these calls often use Voice over Internet Protocol (VoIP). As a result, even when the call agents are in another country, the calls effectively enter the PSTN network within the United States, primarily because this is far cheaper than making an international call. As a result, SHAKEN, even when it is only applied domestically, can begin to have an impact on unwanted robocalls.

Q. **What are analytics? How do they help?**

A. Call blocking apps use artificial intelligence to examine calling patterns and identify likely spam calls. Since these apps use data analytics techniques, they are often referred to as “analytics.” Today, these apps use caller ID data as a key component of their analysis, even though this information can be easily spoofed. SHAKEN will begin to make caller ID information reliable, and as a result will

dramatically improve the effectiveness of call blocking apps. In summary, yes, analytics do help today. In the future, with SHAKEN, they will help even more.

Q. **Will SHAKEN work with legacy (TDM/ISUP) networks?**

A. Generally speaking, no – SHAKEN will not work with legacy TDM/ISUP networks. In specific scenarios, SHAKEN may be able to provide some value for legacy networks that use IP-based interconnection, but this will be limited. To realize the full value of SHAKEN, networks must be SIP-based and use IP-based interconnection.

Q. **Will SHAKEN work for international calls?**

A. Not initially. The STI-GA is defining an infrastructure for calls that originate and terminate in the U.S. However, the SHAKEN protocol has been designed in a way that will allow it to be extended to international calls once other countries adopt SHAKEN. The specific details for a federated SHAKEN infrastructure have yet to be defined, but the base protocol is intended to support this.

For now, besides the U.S., Canada is the only other country that has begun implementing SHAKEN.

Q. **If SHAKEN won't work for international calls initially, won't that defeat the purpose, since the bulk of problem calls are from international sources?**

A. Most problem calls originate from international sources, but these calls typically use VoIP technology and effectively originate as domestic calls, because of the high cost of true international calls. As a result, SHAKEN will have an immediate impact, and as it is extended to apply to international calls, the effectiveness will increase.

Q. **What is it that SHAKEN does not do now that needs a solution? Is it correct that there are some calls that are not getting (SHAKEN) signed by the service provider that should be? And therefore, these "legitimate" calls are not identified to the terminating service provider? (As in the case with those enterprises who use 3rd parties to do their robocalling.)**

A. SHAKEN was never intended to be a complete solution for the robocalling problem. It is an important tool in a multi-layered approach. With that said, what SHAKEN specifically does is to provide "full attestation" when the carrier 1) knows the customer, and 2) has established the right of that customer to use the number. Many scenarios today will not satisfy these conditions and will therefore receive "partial attestation" at most. Third party call centers are a great example of a situation that will not allow full attestation by SHAKEN today, or in any planned evolution of the specification. Again, SHAKEN was never intended to be a complete solution, but an important tool that will move the yardsticks. The DLT use case is an example of the kind of thing that can complement SHAKEN by providing verified information on the intent of the call (e.g., safety recall notice, or flight delay information). Information on the "intent" was never part of SHAKEN. This work is in the early stages of exploring things that could build on top of SHAKEN.

Q. **When SHAKEN is deployed and "legitimate" calls are not identified correctly, these calls might not get delivered?**

A. SHAKEN does not define what service providers should do with the delivery of a call. This is governed by existing regulations that generally (with a few exceptions) require that carriers complete all calls. Note that this does not apply to call-blocking apps, which allow the end user to opt-in and have the app screen, characterize, and potentially block, calls on the user's behalf.

Q. **What percentage of these "legitimate" calls are not identified correctly? If these are a high number, then is SHAKEN useful?**

A. SHAKEN does not characterize calls, and therefore it cannot identify calls correctly or incorrectly. SHAKEN merely creates a digital signature at the origin with the information the originating carrier knows about the call (customer, and potentially their right to use the number) and sends this signature to the terminating carrier, which verifies that no one has tampered with the information. SHAKEN does not identify calls as "SPAM."

Call blocking apps are the entity that tries to identify the call intent, and as a result sometimes label "legitimate" calls as spam. However, it should be noted that call-blocking apps are doing this today. SHAKEN will not make these apps 100% accurate, but it will significantly improve their performance.

SHAKEN is an important foundation for a layered approach to robocalls. The DLT use case is an interesting potential layer to make it important. SHAKEN will be useful as long as it a) improves the situation and b) provides a base that additional techniques can build on.

Q. **What does the terminating service provider do with a robocall that is SHAKEN-signed? Does each terminating service provider follow their own policies? What are some of these? Do some terminating service providers drop the call? Do some terminating service providers add an indicator in the caller ID to indicate that it is a "valid" call?**

A. Yes, terminating carrier actions are left to "local policy". However, this local policy is informed by regulations that require carriers to deliver all calls, except when specifically allowed (currently for, invalid numbers, unallocated numbers, unassigned numbers, and numbers on the Do Not Call list).

Some carriers are planning to provide a "verified" indicator with calls (note, this is not a "valid" indicator) while others are not planning to deliver such an indication. As of today, there isn't industry consensus on what should be displayed to the end user. This topic is currently being hotly debated by the IP-NNI TF.

Call-blocking apps, on the other hand, can do whatever the end user has authorized them to do on their behalf. This is already happening today and has been for some time. Call-blocking apps provide "SPAM likely" indicators, send calls to voice mail, and can even drop calls, if the end user has given them permission to do so. This is different than the network blocking calls, because the end user has explicitly delegated authority to the call-blocking app to act on the user's behalf.

While there is no consensus today, it is intended (hoped) that in the future there will be best practices with broad industry agreement.