Thank you for joining us again. Today's Neustar webinar is, Restore Trust in Phone Calls: Meeting the FCC Call to Action with STIR/SHAKEN. Now, it's my pleasure to introduce today's speakers. We have Jonjie Sena, Senior Director of Products Marketing. Jonjie leads the go-to market strategies to evolve, evangelize, and advance Neustar's Communication Solutions portfolio.

He's joined by Jon Peterson, a fellow at Neustar, co-author of the STIR Standard and resident expert on security and network routing. He is an active member of the Internet Engineering Taskforce, having served as co-area director of transport, the real-time applications and infrastructure area and on the Internet Architecture Board.

With both is Marybeth Degeorgis, Senior Director of Product Management. Marybeth is responsible for the evolution of Neustar's caller identity services, a suite of solutions ensuring secure, accurate, and enriched identity for the voice communications ecosystem.

Thanks, Amanda. Happy Pi Day, everyone and welcome to webinar today. We appreciate everyone joining us to discuss the recent FCC call to action to deploy call authentication and protect consumers. Let me start with something I thought was quite funny. How many of you guys saw John Oliver's latest rant this weekend - which was specifically around this topic of robocalls? If you didn't, I recommend it. It's pretty entertaining, and it's worth the 18 minutes to glance through that.

John Oliver provided what I would view as pretty cool and funny, but consumer-centric, view of the challenges that we hear around robocalls. And I think it's a pretty good summary of many of the conversations I personally have had - both from a social point of view, but even on the professional side as a member of the telecom industry. I think it's a pretty mainstream perspective that will likely resonate with the general public. I'm not sure that I heard anything necessarily new about the issue, but what John Oliver did highlight was several stats that most of us are probably already familiar with. They're all pretty shocking numbers.

We talk about a 57% rise in the number of robocalls, which is already approaching nearly 50 billion this year. We see other stats or projections from other partners that highlight how half the number of mobile calls this year will likely be spam, and even the FCC, as they highlight this as the number one consumer complaint, talks about how over half of their complaints, 60%, are in fact about robocalls.

Most of us are aware of this impact. Most of us are aware of the stats, but this really goes well beyond just the impact on consumers. In fact, the voice services that many of us offer in the telecom world are pretty much under attack, and this affects many different stakeholders and parties. If you walk through some
of the challenges we highlighted here, spoofing not only affects consumers. It also erodes the brands of the businesses that are dialing, or it exposes them to liability when people are actually masquerading as that brand when reaching out to consumers.

**Jonjie Sena:** Call blocking and labeling of calls has been made available to help inform consumers, but there are businesses that are complaining that incorrect blocking and tagging of those calls are in fact happening. Beyond the calls and robocalls to consumers, enterprises themselves are also talking about the incoming robocalls to their businesses. I've not seen any industry stats yet around this, but in conversations with enterprises, we've heard people in the call center space talk about over 10% of the inbound calls to the business, to the agents, are in fact robocalls or potential fraud.

**Jonjie Sena:** Then finally, there's a natural follow-on in the level of distrust in the industry, which is essentially that nobody picks up their calls anymore. That's a big deal because that affects many players. Consumers actually miss important calls that they do want to receive. Enterprises can't deliver messages to customers that are expecting to hear back, and from the operator community, we're seeing an accelerated decline in the use of voice as a form of communication. Further, the operators are being blamed for this negative, fraudulent experience that is impacting voice calls - the most native of communication mechanisms today.

**Jonjie Sena:** Before we dig down into the specifics of call authentication, I think it's worthwhile to sort of break out two really important issues that are very related, but not quite the same thing. Everybody sort of classifies everything we see around the idea of robocalls, and in fact, that's what it is - but if you look at it more closely, robocalls are about delivering recorded messages or the programmatic origination of calls to consumers, whether or not it's recorded or in fact, it's a live person. It is this *programmatic automation* that's essentially allowing the explosion of the numbers of robocalls that we're seeing today. The number is in the billions per month.

**Jonjie Sena:** The second issue is the idea of call spoofing, and what call spoofing is about is the ability for the person that originates the call to change the number so that it appears to be coming from somebody else. In the cases that we see around spoofing and robocalls, there are times when these can really be classified as both legal and illegal. Legal robocalls might be for school closures, weather alerts, or prescription pick-up reminders. In the case of spoofing, legal spoofing is often done to present a main callback number, such as when an agent tries to reach a customer or perhaps show the main hospital number, for when a doctor reaches out to a patient from their own phone number, but they want this to remain private.

**Jonjie Sena:** The illegal calls we see are often a combination of both, so it's the automated dialing with spoofing with the intent to defraud that is the real problem. And
that's really the area that the industry is now actively trying to address. There are different solutions but many of these address this one issue in particular.

**Jonjie Sena:** This brings us to the FCC. I think the top takeaway here is that the Feds are serious in terms of how they're looking at this. In recent press releases and media interviews, FCC Chair Pai has reiterated that stopping robocalls is the number one consumer priority for the FCC, and there are two big initiatives that they've sort of highlighted that are very, very visible to the industry. One is around the area of enforcement. The FCC has started assigning multimillion-dollar fines against robocalls as a deterrent, but when you look at the projections from the various industry groups, we're not really yet seeing a decline as a result of those fines.

**Jonjie Sena:** The second aspect that the FCC has done is they've created the idea of industry pressure, asking the industry to fix it within as part of the solution but also, that if it is not addressed, that there's potential legislation that will force people to solve that issue. Specifically, the FCC actually sent out letters to a large number of the carriers. They did acknowledge that several carriers had already addressed this issue or had at least started, but they also called out specific operators who had not, in their view, made enough progresses - or in fact, didn't have any particular plans in place at all.

**Jonjie Sena:** Beyond the FCC, other lawmakers are also serious about this, and if you look at what's in front of both the U.S. Senate and the Congress, there are activities already aligned to this idea; not only just about enforcement, but around applying policy. In November 2018, the Senate introduced the TRACED Act, which is now in front of the Senate committee for the current session of Congress. And the House also has something similar called the *Stopping Bad Robocalls Act.*

**Jonjie Sena:** A lot of these are focused on the idea of applying penalties for violations of these robocalls. In March, just this month, we've seen a flurry of support from a variety of attorneys General, across 54 states and territories, expressing support for these particular acts.

**Jonjie Sena:** It's not just the regulators. The carriers themselves haven't stood still, and so they've started rolling out solutions. In response to the FCC's November 2017 order to block certain types of calls, many of the leading operators and some of the landline operators have started rolling out solutions to identify robocalls and fraud.

**Jonjie Sena:** These solutions fundamentally use analytics, looking at things like the volume and frequency of calls, who is calling, how many different people are called, seasonality, and many other factors. The consumers are then notified of potential robocall or fraudulent calls. Some carriers are blocking calls, but most of these are done within a very tightly defined category of calls that are either
There is tension between the operators and the businesses making these calls because some of these analytical efforts, in some views, are stopping legitimate calls. The call origination industry has talked about an additional drop of about 20% as a result of these efforts. They feel this is because there is no standard approach to mediate or to correct the mislabeling and tagging of phone numbers. There are many other forums that are already actively involved in this that Neustar is both involved in and have observed. In parallel, beyond this analytics angle, there's also been a lot of work done in the area of call authentication. That's what today's session is all about, this idea of call authentication.

Neustar hosts the ATIS Industry Robocall Testbed, which is about bringing together all the players that offer services and ensure that as they deploy this certification technology, which Jon will highlight in a lot more detail, that it has to work, regardless of what carrier originates the call and what carrier terminates the call.

In the last six months, we've seen a dramatic rise in the number of participants that have signed up, but also in the amount of testing, and this obviously corresponds to a lot of the FCC activity and the regulator angles. You'll see that a lot of the players in the operator space, as well as solution providers, are very active in this organization.

For their part, the operators are doing the testing, but a lot of the feedback has been, "Okay, testing is good, but when will this be available?" This is really a relatively new area. CTIA provided a quick summary based on the FCC ex-parte comments and outlined several of the operators that have identified timelines. You'll see that most of them began work in 2018. Many of them have expressed ongoing work to meet, or even beat, the FCC timeline of the end of the year. This isn't the only set of operators that provided comments. There were many others as well, but not all of them had identified a timeline.

Now, in contrast to the analytics approach, this is really a slightly different approach. This is the idea of using certificates. Specifically, this is to target call spoofing, and it's about using digital certificates to attest to the identities of the caller so that you can identify the person, or not, depending on how the call was originated. Once deployed, this will enable notification to the end user, allowing them to make the decision of whether or not to answer the call.

This is not just about call blocking, this is also about identifying legitimate calls. It's very important to understand that STIR/SHAKEN and call authentication is
really a complement, rather than a replacement, for the other ongoing robocall mitigation strategies in place today.

Jonjie Sena: This takes us to our first viewer poll. We're asking the audience to give us feedback. For those of you that offer these services, which robocall mitigation techniques to-date have been most effective for your subscribers?

We'll start the Jeopardy stop watch and give everybody about 15 or 30 seconds to respond.

Jon Peterson: Should one of us do the tune? (singing)

Jonjie Sena: All right. Let’s see how many we have here. Jon, if you take a look at this, there’s really a variety of different solutions that people have used. Most of them have been through some type of systems and not necessarily customer service, but there’s also a very large percentage, about half actually have either not deployed, or maybe they haven’t found them effective at all, I think is what that might say. Did you have any takeaways from that?

Jon Peterson: Well, we hope we can do better.

Jonjie Sena: Well, that’s a perfect lead in, so let me transfer this over to Jon.

Jon Peterson: Okay, well thank you, and thanks for coming to talk about one of my favorite topics, the STIR/SHAKEN effort. I'm Jon Peterson. I've been heavily involved in STIR/SHAKEN from its inception. In fact, you can blame me for naming STIR when we called the first meeting that led to the STIR work, which I think we held at Google in D.C. in 2013. This was something that the CTO of the FCC approached me about, around that timeframe, and just basically said something needs to be done at a standards level beyond the kind of tactical approaches that people are attempting. We need a foundational technology that these other solutions will be able to build upon.

Jon Peterson: And I think what we'll find as we go through this is that that is what STIR/SHAKEN is going to provide. It's going to provide an approach that will make the existing mitigation techniques much more effective.

Jon Peterson: So, I pose this question. Which is more secure, the telephone network or the internet? 15 years ago, I think we would have answered that one way. I'll just say a lot has changed since then in terms of both how the internet and its security have evolved, and how the telephone network has, in some ways, not really caught up with the times. The telephone network certainly used to be secure. It was so secure because it was effectively a closed network. There were a set of licensed carriers internationally, with access to the underlying signaling network, the SS7 network. That's what we called it. And it was a closed network.
Jon Peterson: And then we can contrast that with the internet in the dark days before the universal adoption of SSL and TLS, or the kind of email spam prevention solutions that we have today. The internet was kind of a wild west where you couldn't really trust anything very much. And then, unfortunately, came along a set of people - and I admit I played a small role here, so I have my share of blame in this as well. We tried to figure out ways to connect the internet to the signaling network, the telephone system. And this resulted in an amazing amount of innovation and disruption, but it had what we call in the technical business, some unanticipated consequences.

Jon Peterson: The problem was that when you interconnect Voice over IP networks with PSTN, it just helped to enable virtually untraceable, abusive phone calls. The protocol we designed to interconnect telephone calls and internet like SIP, borrowed a lot from the way emails were done. And just like with emails, you have a ‘from’ header field, where you can pretty much put whatever you want.

Jon Peterson: We stole that and basically jammed it into SIP calls. Because of that, with SIP, you can just arbitrarily populate the ‘from’ header field and show any name or telephone number - or whatever you want. There wasn't really any way, if it was a telephone number, to verify on the internet whether you have any right to be calling from that number.

Jon Peterson: And the devices we created that connected the internet, practically speaking, to the telephone network, they just looked at the calling number that the internet is telling them and plug them right into the telephone network. And that enabled number spoofing. It's not that there hadn't been number spoofing before that internet connection happened, but this made it cheap, easy and almost untraceable. That is obviously a huge enabler for all these illegal robocalls. The problem is that it's easy and cheap to do it, and if it's untraceable, people are going to use this technique.

Jon Peterson: That is what I'm trying to atone for today. I'll talk a bit about what the plan is. So, what's the plan? Step one of the plan is to bring together the best of internet and phone security. The parts of internet security that keep eCommerce secure today. All things considered; email commerce is pretty much as secure as the telephone network used to be. Now, when you connect to Amazon, you know you’re connecting to Amazon. There's a secure connection. It's not going to be the protocols that you're connecting over that are going to cause any problems for you when you're connecting with Amazon.

Jon Peterson: The way that we do this is we need to have some way then of knowing whether someone has any right to use a given caller number. The best way we know of to attest to an identity on the internet is with a digital signature. Digital signatures could be used in this new framework to issue to carriers or other people who own or are perhaps assigned dedicated telephone numbers, and
they can be used to sign these Voice over IP calls and SIP calls in a way that can be verified by the calling party. So, you know when the numbers being spoofed.

Jon Peterson: Really, we just stole these ideas from the way that web PPI works from the classic X.509 certificate, the same ones you use when you connect to Amazon and it tells you what's on the other side of www.amazon.com. We're going to do the same thing to validate telephone numbers, and related telephone number identifiers.

Jon Peterson: This is where STIR comes in - Secure Telephone Identity Revisited. We say it's revisited because we've been trying to address this, really, since we first started interconnecting these systems together; but nothing much happened until the urgency that Jonjie was alluding to. Regulatory agencies experienced the fury from consumers over this issue and that is when we really felt that we needed to go back and do this in a way that was going to be more conducive to a real solution.

Jon Peterson: This is the logical picture of how STIR works. It's a very high-level overview, but there's a logical authority at the top. It is the logical certificate authority who grants these credentials to a group of new services that you imagine are going to live in the telephone network. There's going to be an authentication service and a verification service. And the authentication service uses a certificate that gives it authority over a telephone number, or over other telephone network identifiers, which sometimes they'll use to assign the call, or assign a SIP request.

Jon Peterson: It then travels through the network, and when it reaches a terminating network, it gets handled by this verification service. The verification service can acquire the public key that was used to assign the call and validate, "Hey, this tells me exactly what I need to know. That the carrier who originated this call is the right person to do it."

Jon Peterson: We usually imagine it's going to be network intermediaries run by carriers who are going to do these functions, but we are also making allowances in the way we design the standards. Where all sorts of end points and potentially, enterprises can be participants in this. There can be a PBX endpoint in the middle of this. Maybe there's a way for enterprises to get their own certificate, to kind of bring them more into this ecosystem.

Jon Peterson: Then there are these 'end points', and we all carry around very smart end points in our pockets today. They talk PKI and do all these things on the web and with email. All the security implements that we need for these services are present on those devices. And SHAKEN is a profile of STIR that was developed by ATIS, which is an industry group of carriers and vendors here in the United States. SHAKEN really defines how you apply that high-level architecture, shown in the
previous slide, to the practical pace of the way carriers communicate with one another over SIP today.

**Jon Peterson:** The same fundamental concepts you see here, the authentication service and the verification service, are present. If you have a call, say from particular number like 202-456-1000, and let's say it is originating from carrier A, that carrier will have a certificate that authorizes it to sign for that number. When the call then arrives through whatever amount of fabric it needs to go through the middle, carrier B can use its verification service to determine that yes, in fact, calls from that number are supposed to be coming from carrier A. And they can notify end-users to tell them that it looks legit.

**Jon Peterson:** If you want some light reading, maybe bedtime reading if you're having trouble getting asleep, here's a good place to start. The STIR standards are defined in an international body called the Internet Engineering Task Force or IETF. It was famous for shepherding the RFC, the Request for Comments series, which defines email, the web, DNS, IP addresses - all that core internet stuff, as well as things like SIP.

**Jon Peterson:** The main RFCs related to STIR are RFC 8224 through 8226, which define things like the sign token you carry in calls, which is called the passport. As well as the certificates that you use to sign those passports, and ultimately validate them on the terminating side. I personally have some small part in putting those three together. The ATIS work defines SHAKEN, including all the operational and policy considerations. The carriers need to understand this in order to implement the STIR architecture more concretely for North American use. Neustar has been very involved in SHAKEN development as well.

**Jon Peterson:** As Jonjie mentioned, we've been running this test lab for ATIS, which is kicking the tires on this and showing that this is real. When people talk about this coming out in 2018-2019, this is because we see a lot of testing implementations happening, and we're beginning to see a certain amount of deployments out there as well.

**Jon Peterson:** Okay, so that was step one. Step two is actually making it happen. Yes, we have these wonderful standards. Everyone likes to write documents. Making it happen is tough. Changing the telephone network is not something that’s easy to do. It’s a pretty ‘baked’ piece of technology. There are a lot of legacy systems and it’s kind of difficult to find the investment to pay for doing major surgery for something like this. So, we're really pushing for a more incremental strategy.

**Jon Peterson:** There’s tremendous regulatory and social pressures, as Jonjie alluded to, to eliminate illegal robocalls, and really the best way to get started is to get involved. It’s to support industry efforts around standardization and testing, to make sure this will work for you and your vendors. This is not something any individual company can do on its own. This is a highly collaborative
environment, which is taking place internationally, that is getting into how these things work.

**Jon Peterson:** And finally, it's important to remember; as I said, this is a foundational technology. Once you manage to prevent spoofing, once you manage to prevent people from being able to impersonate other numbers, that is then the hook that things like analytics can use to ascertain whether or not you should pick up the phone and give you the information you need for that. Marybeth is going to speak about that in just a few minutes here.

**Jon Peterson:** Step three is making sure that we actually solve the issues with the plain old telephone system, because there's more to life than SIP. Depending on how you measure it, something like half of residential deployments today are IP connections for telephones, rather than the kind of black phone, traditional type telephone service. Despite that, most telephone calls do hit the PSTN at some point in their life cycle. And you can lose these fancy signatures, these passwords, that we attach to calls when that happens.

**Jon Peterson:** So, to fix that, we're working on something that's called the STIR out-of-band mechanisms that help preserve the signature, even when the call does not go IP. And then someday, maybe even your smart phone will be able to retrieve these passports itself. We will have a direct security relationship with a calling party, which I think would be really cool, and is something that enterprise call centers, for variety of reasons, are very interested in today.

**Jon Peterson:** And that's the final step that we'll talk about today, which is solving this problem for enterprises. SHAKEN is a carrier-centric standard. It's a profile of STIR that tries to figure out the right way for carriers to implement that on what they call the IPNNI, the network to-network interface the carriers have established for exchanging SIP with one another. But enterprises in some cases also have their own significant SIP infrastructure. And moreover, they want to have a branded display for their customers. They want to be able to reach out with them with logos and so on. So work is underway.

**Jon Peterson:** I actually just wrote a new thing about this. It came out Monday on delegation features for STIR/SHAKEN. This is something that's still coming down the pike, but this is the way carriers will be able to delegate authority for a single telephone number down to an enterprise. The enterprise then will be able to have the significant SIP infrastructure that's required, and many large enterprises already have this in place today. They would then be able to sign these calls themselves, while also using some of the rich call display features that we're designing in compliment with STIR. They'll be able to render all kinds of amazing logos on smartphone screens, and things that just help consumers feel confident when they pick up the phone. So, they know they're actually being reached by the right party.
Jon Peterson: What we hope to get from this is an identity platform that brings telephone numbers into the 21st century.

Jonjie Sena: Thank you Jon, and that really takes us to our second set of polling questions, which essentially asks the audience, “At what stage of implementing call authentication, specifically STIR/SHAKEN, are you today?”

Jon Peterson: Jeopardy music playing. If you can hear the jeopardy music in your head, then you don't need me to do it.

Jonjie Sena: Another five seconds and we will show the results. Let's see what the audience has to say.

Jon Peterson: That's what I'm interested to see. Hmm. Well, I'm thrilled to see some people completed it. Fantastic.

Jonjie Sena: I think if you look at the testbed activity, if you look at the conversations we’re having with carriers, this is very common. This is kind of expected. In many cases there's a couple of people who say they have started, and very few that have completed. But there are those that are near completion. We've heard some of those announcements, but the fact that now is what are you talking about here? People who are just ‘talking about it’ are at 20% right now. Those that either are in progress, or nearly complete, add another 25%.

Jonjie Sena: I think the part that's kind of interesting though are the 21% who have no plans right now, in terms of providing STIR/SHAKEN. I think a lot of the pressure coming from the regulatory side who are looking at those last two areas. That's about half, roughly, who say, "Where is this?" Because in the end, this works when everybody plays.

Jonjie Sena: I'm going to go back and reiterate Jon's encouragement for people to not only adopt, but to participate in, a lot of the collaboration that's ongoing right now.

Jon Peterson: Sure. This is a tough problem. Nobody can do this alone and I think the more of a critical mass we get behind this the better. I mean, it's heartening for me to see how many people are at least pushing forward with it. But if you haven't jumped in yet, join us. The water's warm! It's going to make consumers very happy.

Jonjie Sena: Wonderful. So that takes us in right over to Marybeth's area. Marybeth, off to you.

Marybeth: Thanks, Jonjie. Thank you and good afternoon everyone. Thanks for joining. Again, my name is Marybeth Degeorgis. I am on the product management team here at Neustar. I've been here for a little over 10 years, and all of that time I've
been developing new products and services and rolling those out, which is what I love to do.

Marybeth: Our philosophy here at Neustar is that rather than block all the calls that may in fact be legitimate, or wanted by the receiving party, it’s more prudent and probably beneficial in the end for dialers and receivers of calls to deliverer identity and context. This gives subscribers control over their phone experience. And frankly, just restores trust in calls, protects the consumer, improves customer engagement, and at the same time, protects those dialers; those outbound business dialers that Jonjie talked about. I’ve seen them experience a 20% decrease in connecting with their customers.

Marybeth: And Neustar has a unique perspective here. The reason for that is we sit in kind of a centralized base within the industry. We are the provider of caller identity services to over 90% of the market. We have a ‘hub’ position where we feed over 850 carriers identity information about who's calling. We also feed all of the mobile network and analytics program providers that we've been talking about. Those who’ve introduced some robocall solutions over the past couple of years.

Marybeth: And so, it gives us a unique position, even beyond being a pioneer in call authentication, as Jon has indicated. We also are a trusted steward to the top 7,000 leading global brands, where we manage and provide identity services to brands as well. Being in the space between carriers and brands kind of gives us a unique perspective, and we've been taking these insights over the past couple of years to develop what we think are really great solutions in the space.

Marybeth: We call this our Trusted Call solution suite, and we have developed a number of solutions to meet the challenges that Jonjie and Jon have been talking about. We have our robocall mitigation solution, which applies analytics to detect and block and warn consumers about the type of call they're receiving. We also have a commercial solution in the STIR/SHAKEN arena. I'll talk about each of these in a little bit more detail.

Marybeth: We also have two other new solutions. Caller Name Optimization, which opens what we also all call the ‘old-line’ information database. This provides the ability to identify yourself in the phone network, directly to business customers. We're also very excited about Branded Call Display, which is the ability to deliver additional content and context about who's calling.

Marybeth: So, let's start with our Certified Caller solution, since we've been talking about STIR/SHAKEN along the way. Certified Caller, what Jon and Jonjie have so eloquently described, is commercially available to operators and vendors today. In fact, it's in service at a very large mobile network operator. We will also have an exciting announcement next week about the wider availability of this solution to carriers. So, stay tuned for that.
Marybeth: Basically, Certified Caller is a commercial solution. It can be offered as a standalone, on-premises product for operators supporting IP, and for operators to license and to manage in your own private cloud environment. And then there's also a solution in the cloud on Amazon Web Services. All are using the same solution that was being used in the test lab - and that has been tested by multiple carriers and vendors thus far.

Marybeth: Also, we have a solution called Robocall Mitigation. Robocall Mitigation basically uses analytics to detect and warn customers of unwanted or fraudulent calls. It's set up on the existing caller name infrastructure, and it's easily deployed - at the flip of a switch on the Neustar side. It's widely available to those 850+ carriers that use Neustar for Caller Identity today. What it's doing is using the current infrastructure to overlay the caller name response with an indication of what that call might be, indicating whether it's fraudulent, a robocall or a spammer, etc.

Marybeth: It supports the FCC blocking order that came out in November 2017. It detects if the call is invalid, if someone else has the assigned number, or if it's an unallocated number. These would all be labeled as a fraudulent call. It also has a flexible policy engine. Today, some of you may have a service where you see the spam question mark in front of your caller name when you have an inbound call. That service is powered by Neustar, and that is there because that particular operator set the spam question mark as their policy, but each carrier can set their own policy based on what their internal regulatory or legal departments might direct.

Marybeth: It also supports 'Do Not Originate'. We have many business dialers who might publish a number on the internet that they use for inbound calling only, and therefore it should never make an outbound call. Unfortunately, spammers and scammers have been overtaking these numbers, sometimes using them to demand money from unsuspecting people, saying, for example, they need to pay up or they'll have their utilities turned off. We have the capability to mark those telephone numbers as ‘do not originate’. So, when a spoofer does take over the number to make a call, what a subscriber will see on the receiving end is that this is a fraudulent call.

Marybeth: It also allows for legitimate dialers. Jonjie talked a little bit about the false positive overlays that are happening with some of the solutions that are out there today. This allows legitimate dialers to claim themselves and let themselves be known. Not only within the Neustar service, but because of our hub position, we then share that data out to our carrier partners, as well as the other analytics providers. And so, they can add those legitimate dialers into their analytics as well.

Marybeth: So how does it work at Neustar? Well, we spent over a year with 201 operators developing a pretty solid model. What we do is we incorporate authoritative
industry data. You can envision different types of data for example, assignment data, word data, and we take this data and we meld it with the over 11 billion transactions that we see traversing over our network every month in the caller identity space. We also have something very unique called our One ID database. This is the database where we maintain identity on behalf of those thousands of enterprise customers.

Marybeth: Because we have that OneID data, we know who the legitimate dialers are, and we can incorporate them into our model so that they are no longer falsely identified as a spam caller. In addition to our model, which we refine constantly by the way, we also have an optional dashboard. We have some customers who may not have a centralized means of doing analytics and deep dives into the fraud that might be traversing their network. This dashboard allows them to look at the fraudulent traffic coming into their network and allows them to look at the fraudulent traffic that may be originating on their network, and dive down to the telephone number level to see the patterns and chaos that that particular caller might be causing within their network systems.

Marybeth: We also have Caller Name Optimization which further supports the trusted call experience. It actually allows enterprises to directly manage their brands. Our experience is that identity data can erode rather quickly. In fact, 60% of data is outdated within two years. You can see how that can happen, because 75 million consumers change their carriers every year, 45 million change their telephone numbers, millions of businesses either go through an acquisition or they may close their doors entirely. It's very difficult for carriers to keep up the data.

Marybeth: By allowing these businesses to manage this information directly, it leads to a more accurate and secure data experience. With caller name optimization, a business is actually able to standardize their caller name or customize it by department. The updates are made on demand. They can, as I mentioned, register verified business numbers. So that they get shared with the telecom ecosystem and other analytics providers know that these are legitimate dialers. It also allows you to blacklist numbers.

Marybeth: Envision you’re a utility company or an electric company and you have an inbound only call telephone number. There are, in fact, instances of spoofers taking over these calls and demanding payment on utility bills—whether it's through a gift card scheme or some other crazy means and impersonating this utility. But if that utility has their number marked as 'do not originate’, if the spoofer took that number over, the subscriber would see it as a fraudulent call. This allows businesses to protect themselves in a way by marking some phone numbers as ‘do not originate’ while we wait for the STIR and SHAKEN standards to further solidify in the marketplace.
Marybeth: And then finally, we're very excited about the evolution of Caller Name Optimization, which is branded call display. This is a really exciting initiative to deliver rich content and context about who's calling the mobile device. It helps customers understand why you're reaching out, increases the chances of the call being picked up. The end game is that by providing more information, people will be more likely to pick up the phone. A good example is a cable company coming to visit your home. Many businesses have a bring your own device type situation, and so if this cable person is calling you, you might see just a telephone number on the screen that you don't recognize - and you may not answer it. This causes the cable company to have to re-roll their trucks.

Marybeth: But it's not just cable companies, right? It's services in general. GE is coming to fix your appliance; you typically don't know that it's GE when you see it on your telephone. You'll typically see a telephone number- or maybe you are in a city or state where even this service is unavailable. What Branded Call Display does is it allows enterprises to load additional data so they can put pictures and logos, and even the intent of your call. This helps improve contact rates, reduces the number of dials, and of course, improves the customer journey.

Marybeth: The second picture is all about engagement. Just imagine calling your customer and having your business card show up, or the intent of your call show up. It's much more likely that someone's going to answer that call - and it will elevate the customer experience. We're very excited about Branded Call Display. We currently are piloting this with a select number of enterprises and mobile network operators, and we anticipate we'll be piloting this for the next quarter or two and hope to have this service out into production later this year.

Marybeth: Even more exciting for carriers of course is that this is a new revenue stream. Enterprises are willing to pay for these displays to their end subscriber because it operationally saves them a lot of money to be able to reach someone the first time they're trying to call. And then finally, why Neustar? Well, the final slide summarizes our differentiators, specifically around Caller Intelligence solutions and our ability to combat illegal robocalls and spoofing. And more importantly, we're pioneering call authentication as you've heard from the other speakers on this call.

Marybeth: We have a wide suite of solutions. We aren't just working on one solution. We're working on the entire call experience and call ecosystem, so it's about trusted calls - not just for our carrier customers but for our enterprise customers, and for subscribers in the end. Of course, for carriers, the exciting part is you are anticipating probably having a revenue stream around these trusted call solutions - but brands are very anxious to sign up for these solutions and will pay to reach their customers. So, we're pretty excited to support that.

Marybeth: And with that I think I'll turn it back to Jonjie.
Jonjie Sena: Perfect, thank you Marybeth, and that's just a perfect lead-in to the final poll of the day. The question we're asking the audience is, “what is the most important driver to your organization for implementing call authentication?” We'll give everybody about 15 seconds.

Jonjie Sena: Let's see where we end up. Wow, it's pretty even across the board. What do we see here? We're seeing a third, a third, a third. That's from a regulatory compliance point of view, from a customer care or retention point of view and from the customer experience point of view. I've got to say that having been engaged with a lot of the enterprises and the operators, this is actually not surprising. I think a solution to address trust in phone calls really hits multiple stakeholders within both the operators, as well as the enterprises, and I think this is reflected.

Jonjie Sena: I think the only thing I find fascinating is that risk and security was a zero out of the people that responded. In many ways, this project started as a risk and security mitigation initiative. What do you think, Jon?

Jon Peterson: Well, I think the enterprises are probably the people who are most engaged in the risk and security dimension of this, and this is another area where Neustar has some significant and interesting products designed to help enterprises manage inbound fraudulent calls. But there are a lot of different technologies that go into that. I think it'll turn out STIR/SHAKEN is a good enabler for beating those problems as well.

Jonjie Sena: It's funny, Jon. Let me make a correction. I'm not sure what people are seeing. We have two screens that are slightly different metrics on the one that I have and the one right next to me. Risk and security is about 10%. So, you are starting to see a spread, but I don't think there is one specific group that is well ahead of the game. This has regulatory compliance written all over this as the initial driver, and this is what we've seen based on the pressure from the regulators and the FCC. It also involves many other groups within the operator as well as the enterprises themselves, to sort of solve this problem. Not just from a security point of view, but also from an engagement/retention angle. This is not just from a customer experience perspective, which is I think a lot of the thoughts that we've heard from many people we engage with.

Jonjie Sena: So that's informative, and yet I think in some ways, expected. That kind of brings us now to the Q&A session. We probably have about 12 minutes left before we're done. We already have a lot of questions that have come through, but please continue to write in new questions. We'll try to address as many as we can right now. One of the common questions is “are the slides available” and all of this stuff? The short answer is that post webinar, we will provide a copy of both the PDF of the slides as well as a live recording. And that'll be available to everyone that registered and attended. So please, pass that along to your colleagues.
Jonjie Sena: We will also collate all the questions that we weren't able to answer and update. We typically provide an updated FAQ - but we'll highlight what was new for the webinar and point you as well to the resources that hit all of the Q&A that we've seen. This impacts many different groups: the regulatory view, the security and risk view, the marketing and customer care view. I think that'd be very educational for most.

Jonjie Sena: So that's it. I'm going to start picking through a couple of the questions that have come through. Let's see what we have here. So, the first question I have here is, “What does a carrier do that only has traditional TDM trunks and not SIP trunks?”. I'm going to open it up to either of you, MaryBeth and Jon. Jon, do you want to take a stab at that first?

Jon Peterson: That might be a Jon question. I think MaryBeth certainly should chime in to say that we do have analytic solutions that are available in kind of the STIR/SHAKEN world. I think the STIR/SHAKEN story for how you get those carriers to engage is this out-of-band technology that I referred to. There are a variety of ways that they can engage. For example, gateways can be put in front of legacy infrastructure. These are used to kind of bootstrap your way into a STIR/SHAKEN solution and will still let your calls show up as being valid signed calls at their destination.

Jon Peterson: And to the degree that inside any legacy system, the endpoints or intermediaries have access to the Internet. They too can participate in this kind of out-of-band infrastructure. We're very sensitive to the fact that this needs to work for all the places where the pain really is, right? And a lot of the pain comes from these calls. It started in the IP world and ends up in the PSTN world -and that's precisely what this out-of-band STIR design is there to address.

Marybeth: If I could just add to that; the robocall mitigation solution that Neustar has on its current caller name infrastructure is specifically targeted to TDM, and so it is one of the only solutions I think out there that actually works on the plain old telephone (POTS) service and helps grandma at home. So that's another option.

Jonjie Sena: Perfect, thank you. I want to move on to another question here, and it says, "The majority of complaints we get are really about telemarketing calls from local numbers." I think this is referring to the neighbor spoofing that we've heard. It says, "In most cases, the originating party owns the calling numbers. Therefore, they would be successfully authenticated. How does STIR/SHAKEN address this?" Jon, want to take a stab at that?

Jon Peterson: Yeah. I mean the good news is today is the wild west for people to use neighbor spoofing, right? There is no way to trace back who those entities are effectively. What STIR/SHAKEN gives you is if you're getting a call that is neighbor spoofed and it is in fact from someone who legitimately owns that neighbor number, you can find them. And again, there's no silver bullet. With the regulatory pressures,
and the laws that are being developed, it'll introduce more punitive measures for people who issue illegal robocalls. They will build on top of STIR/SHAKEN and what it does it provides, like non-repudiation for those calls to ascertain, *yes these are the people that generated them, and this is where you should be looking to find accountability for those.*

**Jonjie Sena:** Here's an interesting question that you have covered in some shape, but they ask, "I received a spam call for a phone number identified as one used in England. Will these options work with international originated callers?" and I'm going to add on a second question, just to collapse some of them. "How are other countries participating in STIR/SHAKEN?" but if you could start with the first one. "Will this options work with internationally originated numbers?" is the first question.

**Jon Peterson:** So, right now in the United States, we're going through a process and this began with the CATA working group last year, to define the trust anchor. The TA in CATA stands for trust anchor. This is specifically tied to the regulator in the United States, and so for countries that are going to be able to sign calls through a framework like what I've shared, they will need to go through a similar regulatory process. Now, I speak occasionally to people at Ofcom. I would not want to presume to speak about their plans exactly, but a number of regulators in Europe are tracking this and I think they're looking to us to see how well it's going to work for us before they make decisions.

**Jon Peterson:** In the short term, it really does depend on regulators or industry groups getting together to create these trust anchors for these other nation states. That is a prerequisite for STIR/SHAKEN. Searching and functioning the way that it does, but the good news is that those people are listening, they're watching and I think if we do manage to get the kind of deployment we imagine we will, even by the end of this year, I would hope that they would act accordingly and accelerate their initiatives.

**Jonjie Sena:** Jon, I'd sort of like to add on top of that. I think with regards to the applicability of international numbers; you could break it out into pieces. Any originating call from another international country still has an ingress point or an entry into the U.S. Network, and so if it does enter the country into a carrier that has the ability to do the signing, it will be able to do some form of signing at that level. Would they be able to do that at sort of an intermediate gateway into the carrier?

**Jon Peterson:** SHAKEN does have a provision for signing what they call the gateway level of attestation, and this is something U.S. carriers do. Bear in mind though that pretty much of what this is saying is “I got this from a gateway. It’s not my customer.” And you really have to then rely on the transitive trust of whatever carrier it was you got this from to know the authenticity of the number. I don't believe that's a strong assurance. When AT&T signs a call with the highest level
of authentication, I say this is my customer. I authenticate this person. I know who it is.

**Jon Peterson:** All of these are useful as inputs to the system and the analytics. That will ultimately be used to decide whether to advise people to pick up the phone, but it's not a silver bullet. That's just a part of it.

**Jonjie Sena:** And I think the other angle is in terms of the adoption of STIR/SHAKEN. In Canada the CRTC, for example, has in fact mandated it be put into effect supposedly by this month. I know there's been some adjustment. Canada and the U.S. have looked at STIR/SHAKEN as sort of the, let's call it, the anointed solution. As the first step in call authentication. But I think you've mentioned - and I've heard Jon talking to other industry groups - that other regulators are closely watching. They've not necessarily specifically identified STIR/SHAKEN as the answer, but I do know that Ofcom, I do know that Australia and India and even New Zealand, from what I remember, they're all tackling robocalls. But I don't think STIR/SHAKEN has been mandated or pushed, from what I've seen. Is that a fair representation of what you've seen, Jon?

**Jon Peterson:** Yeah, I don't believe the international treaty organizations who govern what they called E.164, the worldwide numbering plan, have yet done a mandate for that yet. I'd be happy, honestly, if people just could tackle robocalling in their own country. I don't get a lot of spam from numbers that came to me from England, and an important side note of this too is that call may come to you from England or maybe Russia or whatever, even those with a U.S. number. That's what we want to beat. We want to stop people who are impersonating numbers that you think are your neighbors - or that you think is the IRS, or that you think is Apple calling you. I get that Apple one all the time.

**Jonjie Sena:** Here's an interesting piece, and this is probably both a regulatory and a product question. It asks, "Why flag calls rather than block? Is this just because no ID is foolproof?"

**Marybeth:** From our experience, there were a lot of issues out there with blocking calls. If you sit in some of these industry bodies, particularly on the enterprise side, industry consortiums like PACE you'll hear that businesses are having a really difficult time. CVS is a famous example of being overlaid when they're trying to send you prescription information. You don't want calls like that being blocked.

**Marybeth:** We support a lot of enterprises and nearly 100% of them or experiencing false positives on blocking or false positive overlays, because what happens in these programs is they look at volume metrics and they also look at crowdsourcing to determine whether a call should be dropped. And frankly, it gives anybody the ability to record a telephone number as being ‘bad’ simply from their mobile device. That's just not working out, because you have many in the healthcare industry, for example, who are calling to potentially renew an elderly person's
oxygen supply and their telephone numbers are now being blocked by some of these services, or overlaid as being some sort of spam, when in fact, it's just a high-volume, legitimate dialer.

Marybeth: And so, it's really a dangerous practice, and much more prudent, we believe, to inform the consumer about who's calling and then let them make the decision about whether they want to answer that call or not.

Jonjie Sena: Wonderful - and with that, I think I'm going to sort of break into the other Q&A. We have about two minutes before the end of the hour. Thank you so much for all the questions. Honestly, we're a little bit overwhelmed by the number of questions. I apologize, we're unable to hit all of them, but we do promise that we will send a follow-up from the webinar with the slides as well as a Q&A. The Q&A may take a couple more days after the actual slides because we're going to have to collate and try to sort of collapse the questions. There's a lot of very common questions that we'd like to address as one.

Jonjie Sena: In the meantime, what you see here is the contact information. Feel free to check out our website or send emails for follow-ups. We do have everybody's registration information. There will be a follow-up, but again, thank you everybody. We appreciate everyone's time. I think we're all in this together in trying to address this issue of trust in the phone industry and making sure that this is a system that works for all.

Again, thank you very much and Happy Pi Day everybody.

Learn More

Watch the full webinar here or visit Neustar for more information about our Communications Solutions.