Restoring Telecom Trust

By: Donald St. Denis

Let’s start with the bad news: Unwanted robocalls are killing the telephone. Enterprises struggle to reach their customers—even with calls that their customers want.

The good news is that there are new, emerging technologies that will restore trust in and effectiveness of telephone service.

This article will provide a high-level overview of three of these technologies and the benefits they provide to consumers, enterprises, and telephone service providers. These technologies are:

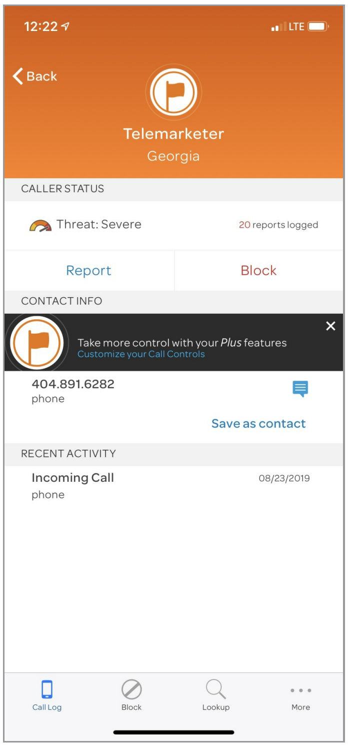
1. Call analytics for robocall mitigation
2. STIR/SHAKEN for caller ID authentication and verification
3. Rich Call Data for secure presentation of branded caller information to the called party

Individually, any one of these technologies can provide some relief from unwanted robocalls. Used separately, though, they leave gaps that clever robocall perpetrators exploit.

The real power of these technologies is realized when they are used in combination. Together, their capabilities and benefits are much greater than the sum of their individual parts.

1. Call Analytics for Robocall Mitigation

One of the first successful responses to unwanted robocalls was the development of call analytics using reputation databases and applications.



12:22 LTE

Telemarketer
Georgia

CALLER STATUS

Threat: Severe 20 reports logged

CONTACT INFO

Take more control with your *Plus* features
Customize your Call Controls

404.891.6282
phone

RECENT ACTIVITY

Incoming Call 08/23/2019
phone

Users load a reputation service application on their mobile phone. When they receive a robocall, the application allows them to report it as a robocall and block the number on future calls *(see Figure 1, right)*. Some apps also identify robocalls by capturing network activity.

Reputation service applications collect reported complaints and suspicious call activity in a central database. After enough complaints or activity, calling numbers used with unwanted robocalls acquire a poor reputation score.

It didn’t take robocall perpetrators long to respond.

They started programming their auto dialer software to construct a random caller ID like the number they were about to call. For example, if the next number to call were 201-555-1234, then the software might construct a caller ID of 201-555-9875. The randomly generated number might or might not be a valid number.

Robocall perpetrators found that people were more likely to answer robocalls when the caller ID number was like theirs. Consumers might not recognize the number, but many thought it could be a neighbor calling, or the school, or their doctor. So, they answered these robocalls. This technique became known as *neighbor spoofing*.

Neighbor spoofing was a stunning setback for call analytics. What good is it to report and block a calling number that was spoofed? That would only penalize innocent subscribers whose numbers had been used in spoofing, not the robocall perpetrators. It’s useless to block a calling number unless you are certain that it wasn’t spoofed. That’s what STIR/SHAKEN is for.

2. STIR/SHAKEN for Caller ID Authentication and Verification

STIR/SHAKEN is used to perform caller ID authentication at origination and verification at call termination.

These James-Bond-inspired acronyms stand for Secure Telephony Identity Revisited (STIR), developed by the Internet Engineering Task Force (IETF), and Secure Handling of Asserted information using Tokens (SHAKEN), developed by ATIS and the SIP Forum.

But don’t worry about these arcane names. The important thing to know is that STIR/SHAKEN is used to prevent caller ID spoofing. Here’s how.

As a service provider is originating an outbound call for its customer, it will use the technology in conjunction with its subscriber information to attest to its confidence about two things:

1. That it knows the customer making the call.
2. That this customer’s use of the calling number is legitimate.

The attestation and related call information is then put into a digitally signed *Identity token* that is sent with the call. This is now a *signed call*.

When a terminating service provider receives a signed call, it uses the technology to verify that:

- The signature is correct.
- The Identity token information matches the asserted caller ID.
- This information hasn’t been changed since the call was signed.

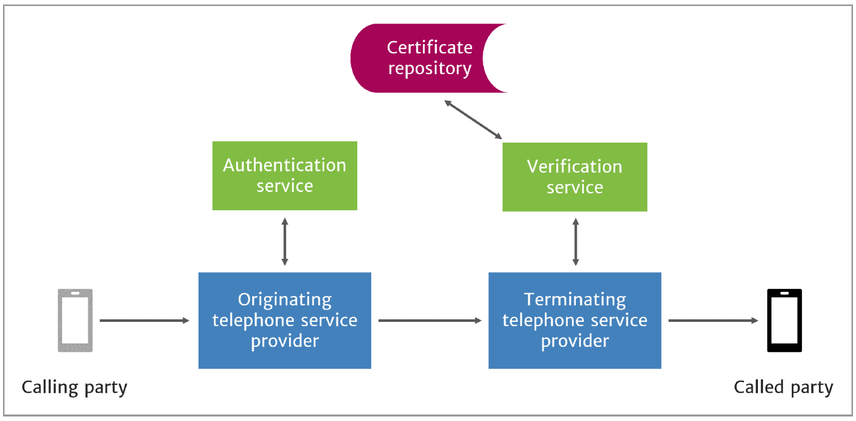


Figure 2: STIR/SHAKEN Network Flow

The service provider then puts *verification status* into the call data, which the handset displays to the called party *(see figure 2)*.

To prevent clever robocall perpetrators from spoofing authentication, the technology uses *Public Key Infrastructure*. The originating provider digitally signs outbound calls with its private key, and the terminating provider verifies these signatures with the originating providers' public key. These keys are associated with *digital certificates*, which are assigned to legitimate service providers by a trusted governance authority. Robocall perpetrators can't get in on it.

STIR/SHAKEN throws new obstacles in the path of robocall perpetrators:

- If a robocall perpetrator spoofs caller ID, then their robocalls will not be authenticated and digitally signed. Terminating service providers will not indicate to their subscriber that the incoming call was verified.
- If a robocall perpetrator replayed or spoofed an Identity token, then it would fail verification and the terminating service provider would apply an appropriate policy to the call (e.g., block or divert).

In the early days of STIR/SHAKEN, before widespread adoption of this technology, most calls will be unsigned and will not raise suspicion. As the technology becomes ubiquitous, subscribers will become more likely to answer verified calls and let unsigned calls go to voicemail.

Regulators and legislators have stated their intention to mandate STIR/SHAKEN if service providers don't implement it voluntarily. Pending legislation and regulations are drafted and ready to go.

But market forces might force the issue. As word spreads about how STIR/SHAKEN identifies authentic caller IDs, subscribers will want it with their telephone service.

STIR/SHAKEN call authentication and verification also makes call analytics useful once again. Unsigned robocalls will land in voicemail. How will robocall perpetrators respond?

They might try to buy inexpensive phone numbers and use them to get their robocalls signed.

Would that work?

Well, their robocalls would be signed. But then crowdsourced reputation applications and other call analytics would eventually catch up with them and assign poor reputation scores to those telephone numbers. The origination ID in the call would enable traceback, a useful tool for law enforcement.

The telephone service that provided those numbers would know that this customer is a robocall perpetrator.

Eventually the telephone numbers would become useless to the robocall perpetrator, and their customer identity would become toxic. The walls would start to close in on them.

Perhaps the most exciting and promising benefit of STIR/SHAKEN is a technology that allows enterprises to introduce themselves to the called party with an authentic representation of their brand. This is *Rich Call Data*.

3. Rich Call Data for Presentation of Branded Caller Information

So far, we have STIR/SHAKEN to prevent caller ID spoofing, and we have call analytics, which are much more effective when we know whether the caller ID was spoofed. Are we done?

Perhaps not.

Telephone subscribers are wary of answering calls from numbers they don’t know. They’ve been burned by too many robocalls for far too long. Even a positive verification status display on their telephone handset might not persuade them to answer a call if they don’t recognize the number.

That’s where Rich Call Data can help. This technology displays the caller name, at the very least, and can also display lots of other information *(see figure 3)*. The framework is currently a draft with the IETF.

Don’t we already have this? Isn’t this CNAM (caller name display)?

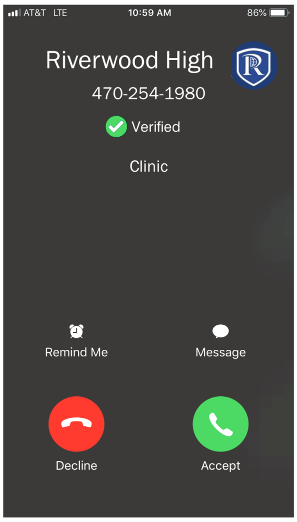
Not exactly. CNAM and eCNAM (enhanced CNAM) are third-party add-on services provided by *terminating service providers*. This means that:

- Not every subscriber has CNAM. Most mobile subscribers do not.
- Since the caller information is collected by third-party services, it’s often incomplete or out of date.
- CNAM often does not display the information the calling party wants to present in the way they want to present it.

Rich Call Data is different:

- It’s built on STIR/SHAKEN. Every consumer who receives signed calls can receive Rich Call Data with those calls, provided their handset will display it.
- Rich Call Data *is produced by the calling party*, not a third party. This makes it much more complete, accurate and up-to-date.
- Since the calling party controls their Rich Call Data, they have greater control over how their brand is presented to people they call.
- Rich Call Data supports more information beyond just display name to help introduce a call more effectively.

Would everyone want to use Rich Call Data? We think so.



Riverwood High
470-254-1980
✓ Verified
Clinic

Some consumers might like the option to have their name put into the Rich Call Data display name field (see Figure 3, right). This might be especially attractive to younger consumers—studies show that they are more hesitant to interrupt or disturb people by making unexpected voice calls. Some might like to have their display name appear on their calls.

Government organizations and schools would find it helpful to improve call answer rates on critical calls.

Rich Call Data can be extremely valuable to enterprises that struggle to reach their customers by telephone. With Rich Call Data, these organizations can present their calls with:

- Display name
- Logo image or picture of the caller
- A variety of data fields supported by the jCard and vCard specifications, including:
  - Identification properties (e.g., name, photo)
  - Communication properties (e.g., telephone, email)
  - Geographical properties (e.g., location)
  - Organizational properties (e.g., title, role)
  - Explanatory properties (e.g., categories, note—such as the reason for the call)

The data supported by the vCard standard is extensive, and handset makers might limit the amount of Rich Call Data they display on their handsets. But this list gives you an idea of the potential scope. Imagine the possibilities!

It’s important to remember that Rich Call Data is an extension of STIR/SHAKEN. This data cannot appear on calls that were not signed. Terminating service providers probably would not present this data for calls that do not pass verification.

This means that Rich Call Data is a more secure, trusted way to introduce a telephone call.

Putting It All Together

These three technologies build upon and complement each other. Together, they are much more powerful and effective:

1. **STIR/SHAKEN** — Prevents caller ID spoofing.
2. **Call Analytics** — Becomes much more effective in preventing robocalls when spoofing is identified.
3. **Rich Call Data** — Introduces signed and verified calls with more information to help the called party feel comfortable about answering these calls.

Together, STIR/SHAKEN, call analytics, and Rich Call Data provide these benefits to allow consumers to feel more comfortable in answering calls that are signed and introduced with Rich Call Data, and enterprises will find it easier to connect with their customers when presenting a branded identity with their calls.

In addition, telecommunications service providers will see:

- An improvement in their call completion rate
- More effective call analytics and robocall blocking
- Fewer complaints about unwanted robocalls
- Increased customer satisfaction and decreased churn.

In short, these emerging technologies will work together to help restore trust in telephone services.