

Amended Exhibit B: Infringement Contentions for U.S. Patent No. 11,005,989 vs. AT&T

Plaintiff RightQuestion accuses Defendants AT&T Corp., AT&T Mobility LLC, AT&T Mobility II LLC, and AT&T Services Inc. (collectively, “AT&T” and/or “Defendants”) of making, using, offering for sale, selling in (including licensing) and/or importing into the United States Defendants’ system(s) and/or method(s) for verifying caller identification information, including Defendants’ Robocall Mitigation, Call Protect, Digital Call Protect, ActiveArmor, caller identification verification mobile applications (for Android, iOS, and/or any other operating systems), and all other of Defendants’ systems, methods, services, products, and/or devices—physical and/or virtual—that implement caller identification authentication and/or verification technology (collectively, the “Accused Instrumentalities”). The “Accused Instrumentalities” include without limitation Defendants’ particular implementation of the caller authentication technology known as Secure Telephony Identity Revisited (“STIR”) that defines a caller signature and “Signature-based Handling of Asserted Information Using toKENs (“SHAKEN”) that provides an implementation to verify the signature, including but not limited to Requests for Comment (“RFC”) 8224, RFC 8225, RFC 8226, RFC 8588, ATIS-1000074, ATIS-1000080, and ATIS-1000084 (together known as “STIR/SHAKEN” or “SHAKEN/STIR”). The term “Accused Instrumentalities” also includes all associated interfaces, software, data, digital content, electronic devices, hardware, and processes and methods related thereto and all associated third-party (for example, Hiya) components, systems, and/or technologies deployed, used, and/or otherwise incorporated in the Accused Instrumentalities.

Defendants have directly infringed and continue to directly infringe 1-28 of U.S. Patent No. 11,005,989 (the “’989 Patent”) by performing each and every step of the claims or making, using, selling, or offering for sale the Accused Instrumentalities which meet every element of the claims, as shown below. Defendants also directly infringe the asserted claims of the ’989 patent to the extent Defendants contracted with, is in a joint venture with, directed, and/or otherwise conspired with a third party to perform any of the steps or provide any element of the asserted claims. Defendants also directly infringe the asserted claims to because any step of a claimed method is attributable to Defendants to the extent, for example, Defendants condition participation in an activity or receipt of a benefit upon performance of a step or steps of the patented method and establish the manner or timing of that performance, or to the extent Defendants control the Accused Instrumentalities as a whole and obtains benefit from them. Defendants are therefore liable for infringement of the ’989 Patent under 35 U.S.C. § 271(a).

Defendants have induced and continue to induce infringement of claims 1-28 of the ’989 Patent by, with knowledge of the ’989 Patent and specific intent to encourage infringement, knowingly and actively providing to third parties including users, customers, agents and/or others the Accused Instrumentalities to utilize in an infringing manner. The Accused Instrumentalities and the operation or use thereof by such third parties directly infringes the asserted claims by putting the claimed systems into use and/or by constituting performance of the claimed methods. Defendants intend to cause infringement by such third parties. Defendants require, instruct, and/or control and direct third parties to use the Accused Instrumentalities in an infringing manner, including without limitation by providing

instructions to such third parties to operate the Accused Instrumentalities in an infringing manner and/or preconditioning use of the Accused Instrumentalities on use in an infringing manner. Defendants further manifest this intent to induce infringement by providing support services for the Accused Instrumentalities, including providing instruction, support training, and services, and actively inducing its customers to sign up for accounts. *See, e.g.,* ActiveArmor, AT&T, RQ-ATT0000035-RQ-ATT0000041 (<https://www.att.com/security/>); AT&T Call Protect | AT&T Cyber Aware, AT&T, RQ-ATT0000054 (<https://about.att.com/pages/cyberaware/ae/cp>); AT&T ActiveArmor and Mobile Security Apps, AT&T, RQ-ATT0000027-RQ-ATT0000034 (<https://www.att.com/security/security-apps/>); Stop Unwanted Calls with Digital Phone Call Protect, AT&T (April 25, 2023), RQ-ATT0000137-RQ-ATT0000138 (<https://www.att.com/support/article/u-verse-voice/KM1235421/>); AT&T ActiveArmor on the App Store, Apple (Feb. 20, 2024), RQ-ATT0000049-RQ-ATT0000050 (<https://apps.apple.com/us/app/at-t-activearmor/id1218465964>); AT&T ActiveArmor - Apps on Google Play, Google (Feb. 21, 2024), RQ-ATT0000042-RQ-ATT0000045 (<https://play.google.com/store/apps/details?id=com.att.mobilesecurity>); Use the AT&T ActiveArmor Mobile Security app, AT&T (Dec. 7, 2022), RQ-ATT0000151-RQ-ATT0000152 (<https://www.att.com/support/article/wireless/KM1147710/>); AT&T and T-Mobile Work Together to Give Customers New Call Authentication Protections, RQ-ATT0000051-RQ-ATT0000053 (https://about.att.com/story/2019/att_tmo_call_authentication.html); AT&T Now Blocking or Labeling More Than 1 Billion Robocalls Per Month, AT&T (June 22, 2021), RQ-ATT0000135-RQ-ATT0000136 (<https://about.att.com/story/2021/robocalls.html>); AT&T Activates Call Validation Displays, AT&T (Dec. 18, 2019), RQ-ATT0000024-RQ-ATT0000026 (https://about.att.com/story/2019/call_validation_displays.html). Where the customers are the direct infringers, the underlying direct infringement occurs, for example, when Defendants provide call verification which occurs when an end-user makes a phone call as described in the claims below. Customers obtain benefits such as call spam, spoof, and fraud protection. Defendants are therefore liable for infringement of claims 1-28 of the '989 Patent under 35 U.S.C. § 271(b).

Defendants have contributed and continue to contribute to infringement of claims 1-28 of the '989 Patent by, with knowledge of the '989 Patent, placing or contributing to placing the Accused Instrumentalities into the stream of commerce knowing or understanding that such products and/or services would be sold and used and knowing such components constitute a material portion of the invention, are especially made or adapted for use in infringement of the asserted claims, and are not a staple article or commodity of commerce suitable for substantial non-infringing uses. Defendants' affirmative acts of providing the Accused Instrumentalities to implement and support the infringing technology for validating and/or verifying caller identification information and causing the infringing technology, services, and/or protocols to be used and implemented by Defendants' customers, other voice-service providers, and/or other third parties contribute to their implementation of infringing verification technology, such that there is direct infringement by Defendants' customers, end-users, other voice-service providers, and/or such other third parties. Defendants are therefore liable for infringement of claims 1-28 of the '989 Patent under 35 U.S.C. § 271(c).

The asserted claims include elements that are implemented, at least in part, by proprietary and specialized electronics, firmware, and

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

software in the Accused Instrumentalities. The precise designs, processes, and algorithms used in them are held secret, at least in part, and are not publicly available in their entirety. An analysis of Defendants' documentation and/or source code may be necessary to fully and accurately describe all infringing features and functionality of the Accused Instrumentalities and, accordingly, Plaintiff reserves the right to supplement these contentions once such information is made available to Plaintiff. Furthermore, Plaintiff reserves the right to revise these contentions, including as discovery in the case progresses, in view of any non-infringement arguments Defendants may make (*e.g.*, to allege infringement under the doctrine of equivalents), in view of the Court's final claim construction in this action and in connection with the provision of expert reports.

U.S. Patent No. 11,005,989	AT&T’s Infringement
Claim 1. [pre] A system, comprising:	This is the preamble of the claim and is not limiting. To the extent the preamble is construed as limiting, the Accused Instrumentalities comprise a system(s) for validating and/or verifying caller identification information as described below. The Accused Instrumentalities, alone and/or in combination, comprise one or more system(s) and service(s) that are configured to perform a security determination and convey an assurance to a callee associated with a given call or convey a failure to confirm to the callee, and/or are otherwise capable of detecting, blocking, and preventing SPAM, fraudulent, and spoofed phone calls. <i>See, e.g., Network & Data Security, AT&T, RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security):</i> • Robocall Scam Identification & Mitigation: AT&T has established mechanisms to identify illegal robocall campaigns and help to mitigate them. ◦ Through the complementary programs listed below, AT&T has blocked or labeled billions of unwanted robocalls. ▪ AT&T ActiveArmorSM automatically blocks fraud calls and labels other suspected spam calls so a wireless customer can choose to answer or not. It identifies the calls through data analytics, network intelligence and customer reports. ▪ AT&T’s Global Fraud Management team works closely with the U.S. Telecom Industry Traceback Group and law enforcement to identify the source of illegal calls. This process provides necessary information to stop illegal robocall campaigns and places responsibility on service providers for traffic that originates on their networks. ▪ AT&T’s Global Fraud Management organization, with assistance from the AT&T Chief Data Office, uses sophisticated algorithms to examine billions of calls each day for patterns that indicate a robocalling scheme. They investigate suspicious activity that may be illegal, relying on human fraud expertise before blocking. ◦ Implementation of the caller ID authentication standard known as STIR/SHAKEN remains a top priority for AT&T, and we have deployed it across our IP networks. We have filed comments with the Federal Communications Commission (FCC) detailing our progress on this front and offering our support as the FCC addresses the complex details of implementation. We also supported the TRACED Act, which codified implementation requirements.

For example, AT&T advertises “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (<https://www.att.com/security/>).

How do AT&T and the other major carriers differ in terms of security? ^

AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.

To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost.

ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited

Req’s compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req’s apply. Details at att.com/activearmorapp.

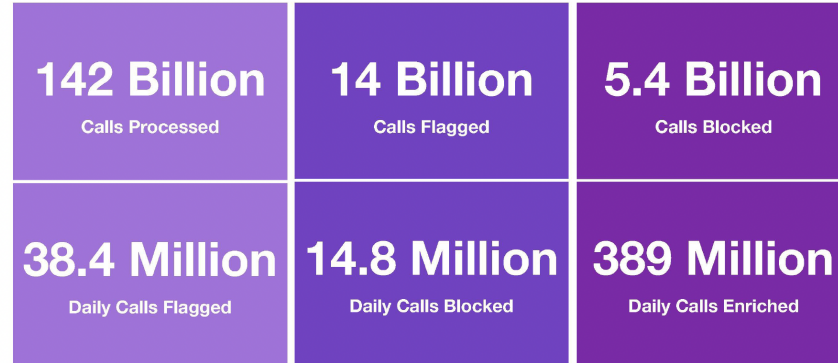
Feedback

CHAT

As another example, AT&T advertises that with Digital Phone Call Protect, customers get “call validation,” “Automatic fraud blocking,” and “Suspected spam call warning,” among other features. *See, e.g.*, RQ-ATT0000137-RQ-ATT0000138 (<https://www.att.com/support/article/u-verse->

	voice/KM1235421/): Digital Phone Call Protect features Here's what you get with Digital Phone Call Protect¹: • Call validation: Soon you'll see a [V] on your caller ID for some calls. This means we've confirmed that the call originated from the phone registered to that number. (Remember to still be cautious when answering a call from an unknown number.) • Automatic fraud blocking: Each potential fraud call gives the caller a busy signal, and the call won't go through. You can toggle this feature on or off. • Call blocking: If you have a specific number you want to block, press *61 after the unwanted call to block that number. • Call log: You can see detailed call log info. • Suspected spam call warning: Your caller ID will show Suspected Spam and a type (Political, Nonprofit, Telemarketer, Survey, or Robocaller). For example, the Accused Instrumentalities comprises one or more processors configured to implement protocols, technologies, features, and services for validating and/or verifying caller identification information including without limitation STIR/SHAKEN. <i>See, e.g.,</i> ATT-RQ_0000001 at 3 (showing volume of blocks calls necessitating the use of computer systems with processors to make the determination to block or connect an outgoing or incoming call):
--	--

Hiya-AT&T Call Protect 2023 Summary



Hiya PROPRIETARY AND CONFIDENTIAL

hiya

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

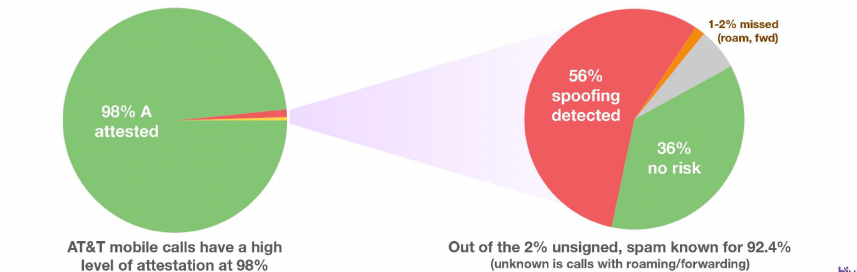
ATT-RQ_0000003

See, e.g., ATT-RQ_0000001 at 26 (showing that AT&T prevents spoofing from its own numbers on its network):

Working with AT&T, Hiya has been successful at preventing spoofing from AT&T phone numbers

STATE OF THE SERVICE TODAY:

Working closely with AT&T, Hiya has solutions in place to address the challenges in mobile spoof detection. Hiya has deployed in production a mobile spoof detection solution that we feel is detecting **98% of spoofed calls using AT&T mobile numbers**, and detecting a large majority of spoofing using other mobile carrier lines.



Hiya PROPRIETARY AND CONFIDENTIAL

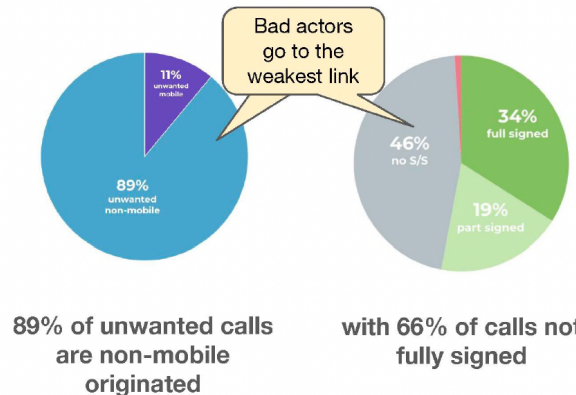
hiya

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

ATT-RQ_0000026

See, e.g., ATT-RQ_0000001 at 28 (noting that call authentication technologies beyond STIR/SHAKEN are required to prevent fraudulent, spam, and spoofed phone calls):

However, the majority of unwanted calls stem from non-mobile sources, and STIR/SHAKEN is far from fixing this issue



STATE OF THE ECOSYSTEM:

Key impediments on STIR/SHAKEN non-mobile spoofing include:

- Unstable Implementation for Non-Mobile Numbers
- Challenges from Legacy Systems
- Incomplete Adoption Among Service Providers
- Verification and Trust Issues

These complexities provide opportunities for scammers to exploit coverage gaps

Calls from non-mobile sources are much more likely to be unwanted compared to calls from mobile sources

28 | HIXA PROPRIETARY AND CONFIDENTIAL

hiya

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

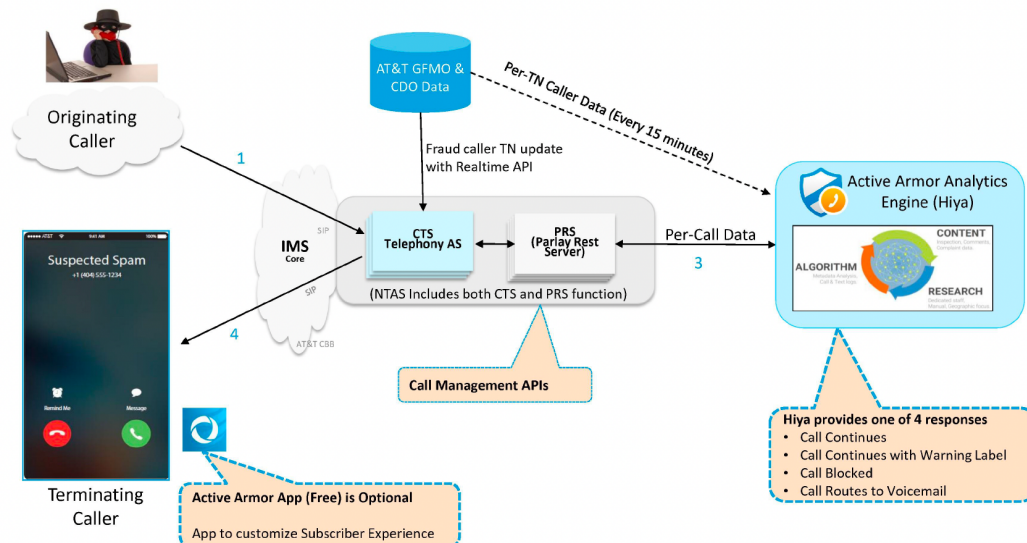
ATT-RQ_0000028

The Accused Instrumentalities are implemented, used, and/or put into service by AT&T in intra- and inter- network communications. See, e.g., RQ-ATT0000051-RQ-ATT0000053 (https://about.att.com/story/2019/att_tmo_call-authentication.html).

	AT&T* and T-Mobile today began rollout of cross-network call authentication based on SHAKEN/STIR standards – another big step toward protecting consumers from unwanted robocalls. SHAKEN/STIR technology lets consumers know that an incoming call is really coming from the number listed on the caller ID display – not a spoofed robocall or scammer. While authentication won’t solve the problem of unwanted robocalls by itself, it is a key step toward giving customers greater confidence and control over the calls they answer. For example, a call that is illegally “spoofed” – or shows a faked number – will fail the SHAKEN/STIR Caller ID verification and will not be marked as verified. By contrast, verification will confirm that a call is really coming from the identified number or entity. More calls will be verified over time as more device providers participate, and as more network providers implement the standards. The FCC has recommended SHAKEN/STIR standards to digitally validate phone calls. The acronym stands for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR). For more information on all the ways AT&T is protecting customers, visit https://about.att.com/story/2019/att_call_protect.html and https://att.com/CyberAware.
--	---

See, e.g., ATT-RQ_0000045 (Hiya provides at least one of four responses – namely, “Call Continues,” “Call Continues with Warning Label,” “Call Blocked” or “Call Routes to Voicemail” (e.g., whether or not the call has an assurance or a failure of an assurance)):

AT&T Active Armor (Call Protect) – High Level Architecture



© 2022 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T companies except under written agreement.

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

ATT-RQ_0000045

As another example, the Accused Instrumentalities implement STIR/SHAKEN, among other protocols, technologies, features, and services for validating and/or verifying caller identification information. See, e.g., RQ-ATT0000024-RQ-ATT0000026 (https://about.att.com/story/2019/call_validation_displays.html):

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

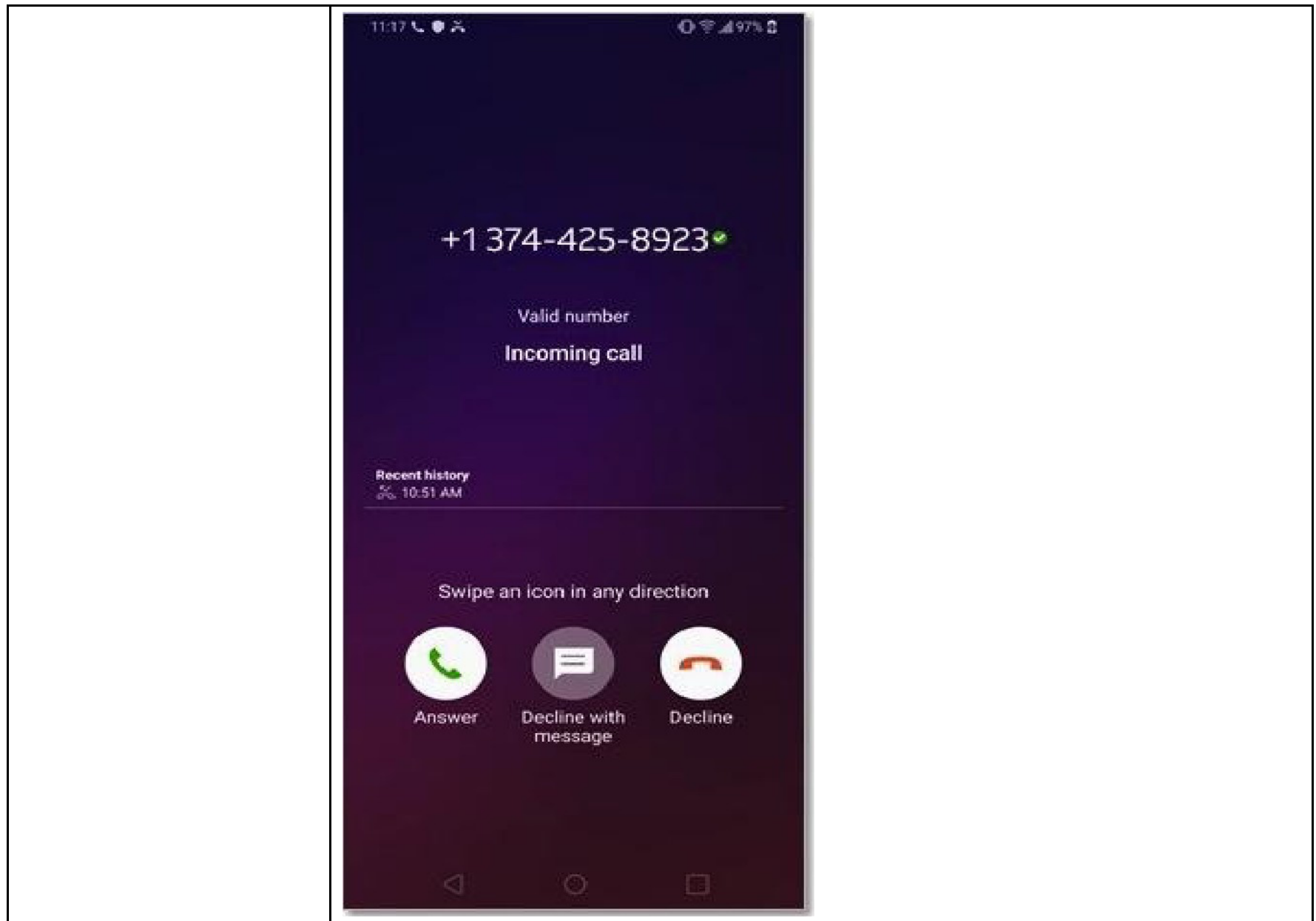
	AT&T* has turned on its first phone displays that let you know an incoming call is really from the number appearing on Caller ID. This fights against “spoofing” of phone numbers – a trick used by many illegal robocallers. Most AT&T customers with a Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ™ will see a special display when an incoming call has been authenticated. They will see a green checkmark and the words, “Valid Number.” Consumers with AT&T Phone digital home phone service also can activate the feature. It will give them a “[V]” for valid number. Phone service providers have jointly developed a technology – the SHAKEN/STIR standards – to digitally validate calls. This won’t solve the problem of unwanted robocalls by itself. But it can give consumers greater confidence and control over the calls they answer. “This is another step to tame annoying, unwanted robocalls,” said Kevin Petersen, AT&T senior vice president, Postpaid Wireless Products. “In the coming year, we’ll continue to take more steps and put more pressure on the bad guys.” AT&T is rolling out its SHAKEN/STIR display as part of its AT&T Call Protect service, which is being added at no charge to millions of mobility consumer lines. AT&T Call Protect blocks or labels suspected illegal and unwanted robocalls. This strategy will give a multiplier effect to call protection: A “valid number” on an AT&T device means the incoming call has been authenticated by SHAKEN/STIR <i>and</i> passed through AT&T Call Protect screening.
--	---

	Here are some other key points: • A call that shows “valid number” has been verified and can increase your trust level. But a call without the label may still be a legitimate call. More calls will be marked with “valid number” over time, as more network providers implement SHAKEN/STIR and link to each other. • AT&T has rolled out AT&T Call Protect automatically to many Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ users. Others are on the way soon.¹ If you’re not seeing call validation on those devices when you accept their latest software update, you don’t have to wait. You can download the AT&T Call Protect app, or turn on the service from your account settings in myAT&T. • AT&T Phone digital home phone users can opt-in to get AT&T Digital Phone Call Protect and call validation. Just go to your account settings on myAT&T and turn it on. • Validation displays will be added to more mobile devices in the new year. • Finally, a “valid number” display helps fight against bad guys, but it can never guarantee an individual caller is a good guy. Consumers should always use their best judgement when answering calls from strangers. <i>See, e.g.,</i> RQ-ATT0000051-RQ-ATT0000053 (https://about.att.com/story/2019/att_tmo_call_authentication.html).
--	--

	AT&T* and T-Mobile today began rollout of cross-network call authentication based on SHAKEN/STIR standards – another big step toward protecting consumers from unwanted robocalls. SHAKEN/STIR technology lets consumers know that an incoming call is really coming from the number listed on the caller ID display – not a spoofed robocall or scammer. While authentication won’t solve the problem of unwanted robocalls by itself, it is a key step toward giving customers greater confidence and control over the calls they answer. For example, a call that is illegally “spoofed” – or shows a faked number – will fail the SHAKEN/STIR Caller ID verification and will not be marked as verified. By contrast, verification will confirm that a call is really coming from the identified number or entity. More calls will be verified over time as more device providers participate, and as more network providers implement the standards. The FCC has recommended SHAKEN/STIR standards to digitally validate phone calls. The acronym stands for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR). For more information on all the ways AT&T is protecting customers, visit https://about.att.com/story/2019/att_call_protect.html and https://att.com/CyberAware. Caller identification authentication and verification technology, including without limitation
--	---

	STIR/SHAKEN, is technology configured to and/or used to, among other functions, detect spoofed phone calls. <i>See, e.g.,</i> RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/); RQ0001970 (https://sti-ga.atis.org/resources/). ATIS STANDARD ATIS-1000074-E -- SIP Forum TWG-10-E ATIS Standard on – Signature-based Handling of Asserted information using toKENs (SHAKEN) 1 Scope & Purpose 1.1 Scope This document is intended to provide telephone service providers with a framework and guidance on how to utilize Secure Telephone Identity (STI) technologies toward the validation of legitimate calls and the mitigation of illegitimate spoofing of telephone identities on IP-based service provider voice networks (also to be referred to as Voice over Internet Protocol [VoIP] networks). The primary focus of this document is on the format of STI claims, the mapping of these claims to SIP (RFC 3261), and the authentication and verification functions.
--	--

	1.2 Purpose Using the protocols defined in ~~draft-ietf-stir-rfc4474bis~~RFC 8224 and ~~draft-ietf-stir-passport~~RFC 8225, this document defines the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework. This framework is targeted at telephone service providers delivering phone calls over VoIP, and addresses the implementation and usage of the IETF STIR Working Group protocols and the architecture and use of STI-related X.509-based certificates (RFC 5280). It also discusses the general architecture of service provider authentication and verification services. Finally, it provides high level guidance on the use of positive or negative verification of the signature to mitigate illegitimate telephone identity in general. Illegitimate Caller ID spoofing is a growing concern for North American telephone service providers and their customers. There are many Caller ID spoofing mechanisms, and illegitimate spoofing can evolve to evade mitigation techniques. Service provider solutions must therefore be flexible to respond to evolving threats in much the same way as cybersecurity solutions. In addition, the integration of new technologies into established VoIP networks imposes many interoperability and interworking challenges. As a result, this document is a baseline document on the implementation of the protocol-related requirements for STI. The objective is to provide a baseline that can evolve over time, incorporating more comprehensive functionality and a broader scope in a backward compatible and forward looking manner.
1[a] one or more processors configured to:	The Accused Instrumentalities comprise one or more processors. Within the Accused Instrumentalities, the one or more processors comprise one or more devices, circuits, and/or processing cores configured to process data, including computer program instructions to perform the limitation of the claim. The one or more processors may be a processor(s) located within Defendants’ network, a third party (e.g., Hiya) processor(s) deployed, used, and/or otherwise incorporated in the Accused Instrumentalities, or some combination thereof. <i>See</i> ATT-RQ_0000001 and ATT-RQ_0000042. For example, the Accused Instrumentalities including without limitation AT&T’s Robocall Mitigation system(s), Call Protect system(s) and service(s), ActiveArmor, and the ActiveArmor mobile application are configured to implement call authentication technology for validating and/or verifying caller identification information, using one or more processors. <i>See, e.g.</i>, RQ-ATT0000024-RQ-ATT0000026 (https://about.att.com/story/2019/call_validation_displays.html):



	<i>See, e.g.,</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security): • Robocall Scam Identification & Mitigation: AT&T has established mechanisms to identify illegal robocall campaigns and help to mitigate them. ◦ Through the complementary programs listed below, AT&T has blocked or labeled billions of unwanted robocalls. ▪ AT&T ActiveArmorSM automatically blocks fraud calls and labels other suspected spam calls so a wireless customer can choose to answer or not. It identifies the calls through data analytics, network intelligence and customer reports. ▪ AT&T's Global Fraud Management team works closely with the U.S. Telecom Industry Traceback Group and law enforcement to identify the source of illegal calls. This process provides necessary information to stop illegal robocall campaigns and places responsibility on service providers for traffic that originates on their networks. ▪ AT&T's Global Fraud Management organization, with assistance from the AT&T Chief Data Office, uses sophisticated algorithms to examine billions of calls each day for patterns that indicate a robocalling scheme. They investigate suspicious activity that may be illegal, relying on human fraud expertise before blocking. ◦ Implementation of the caller ID authentication standard known as STIR/SHAKEN remains a top priority for AT&T, and we have deployed it across our IP networks. We have filed comments with the Federal Communications Commission (FCC) detailing our progress on this front and offering our support as the FCC addresses the complex details of implementation. We also supported the TRACED Act, which codified implementation requirements. <i>See, e.g.,</i> RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/):
--	--

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req’s compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req’s apply. Details at att.com/activearmorapp. Feedback See, e.g., RQ-ATT0000137-RQ-ATT0000138 (https://www.att.com/support/article/u-verse-voice/KM1235421/):
--	--

Digital Phone Call Protect features

Here's what you get with Digital Phone Call Protect¹:

- **Call validation:** Soon you'll see a [V] on your caller ID for some calls. This means we've confirmed that the call originated from the phone registered to that number. (Remember to still be cautious when answering a call from an unknown number.)
- **Automatic fraud blocking:** Each potential fraud call gives the caller a busy signal, and the call won't go through. You can toggle this feature on or off.
- **Call blocking:** If you have a specific number you want to block, press *61 after the unwanted call to block that number.
- **Call log:** You can see detailed call log info.
- **Suspected spam call warning:** Your caller ID will show Suspected Spam and a type (Political, Nonprofit, Telemarketer, Survey, or Robocaller).

For example, the Accused Instrumentalities comprises one or more processors configured to implement protocols, technologies, features, and services for validating and/or verifying caller identification information including without limitation STIR/SHAKEN.

See, e.g., ATT-RQ_0000001 at 3 (showing volume of blocks calls necessitating the use of computer systems with processors to make the determination to block or connect an outgoing or incoming call):

Hiya-AT&T Call Protect 2023 Summary



Hiya PROPRIETARY AND CONFIDENTIAL

hiya

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

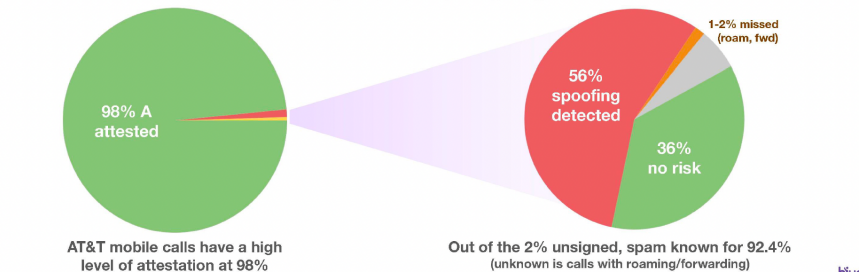
ATT-RQ_0000003

See, e.g., ATT-RQ_0000001 at 26 (showing that AT&T prevents spoofing from its own numbers on its network):

Working with AT&T, Hiya has been successful at preventing spoofing from AT&T phone numbers

STATE OF THE SERVICE TODAY:

Working closely with AT&T, Hiya has solutions in place to address the challenges in mobile spoof detection. Hiya has deployed in production a mobile spoof detection solution that we feel is detecting **98% of spoofed calls using AT&T mobile numbers**, and detecting a large majority of spoofing using other mobile carrier lines.



Hiya PROPRIETARY AND CONFIDENTIAL

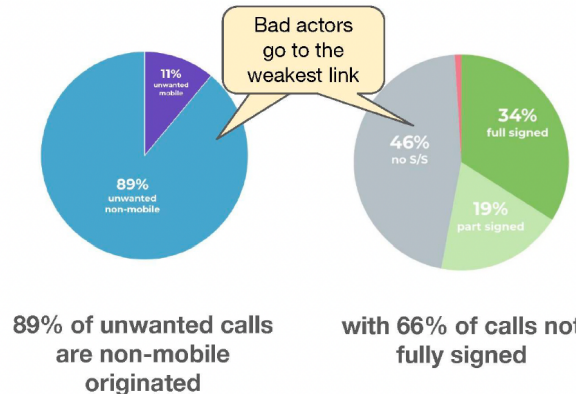
hiya

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

ATT-RQ_0000026

See, e.g., ATT-RQ_0000001 at 28 (noting that call authentication technologies beyond STIR/SHAKEN are required to prevent fraudulent, spam, and spoofed phone calls):

However, the majority of unwanted calls stem from non-mobile sources, and STIR/SHAKEN is far from fixing this issue



STATE OF THE ECOSYSTEM:

Key impediments on STIR/SHAKEN non-mobile spoofing include:

- Unstable Implementation for Non-Mobile Numbers
- Challenges from Legacy Systems
- Incomplete Adoption Among Service Providers
- Verification and Trust Issues

These complexities provide opportunities for scammers to exploit coverage gaps

Calls from non-mobile sources are much more likely to be unwanted compared to calls from mobile sources

28 | HUYA PROPRIETARY AND CONFIDENTIAL

hiya

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

ATT-RQ_0000028

See, e.g., *AT&T Activates Call Validation Displays*, AT&T, (Dec. 18, 2019), RQ-ATT0000024-RQ-ATT0000026 (https://about.att.com/story/2019/call_validation_displays.html).

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

	AT&T* has turned on its first phone displays that let you know an incoming call is really from the number appearing on Caller ID. This fights against “spoofing” of phone numbers – a trick used by many illegal robocallers. Most AT&T customers with a Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ™ will see a special display when an incoming call has been authenticated. They will see a green checkmark and the words, “Valid Number.” Consumers with AT&T Phone digital home phone service also can activate the feature. It will give them a “[V]” for valid number. Phone service providers have jointly developed a technology – the SHAKEN/STIR standards – to digitally validate calls. This won’t solve the problem of unwanted robocalls by itself. But it can give consumers greater confidence and control over the calls they answer. “This is another step to tame annoying, unwanted robocalls,” said Kevin Petersen, AT&T senior vice president, Postpaid Wireless Products. “In the coming year, we’ll continue to take more steps and put more pressure on the bad guys.” AT&T is rolling out its SHAKEN/STIR display as part of its AT&T Call Protect service, which is being added at no charge to millions of mobility consumer lines. AT&T Call Protect blocks or labels suspected illegal and unwanted robocalls. This strategy will give a multiplier effect to call protection: A “valid number” on an AT&T device means the incoming call has been authenticated by SHAKEN/STIR <i>and</i> passed through AT&T Call Protect screening.
--	---

Here are some other key points:

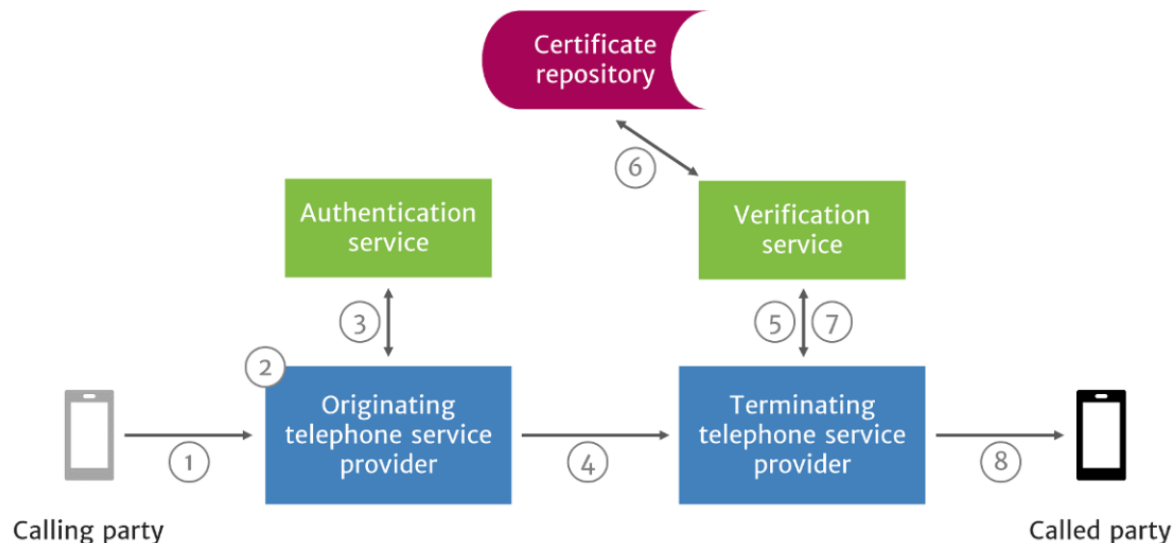
- A call that shows “valid number” has been verified and can increase your trust level. But a call without the label may still be a legitimate call. More calls will be marked with “valid number” over time, as more network providers implement SHAKEN/STIR and link to each other.
- AT&T has rolled out AT&T Call Protect automatically to many Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ users. Others are on the way soon.¹ If you’re not seeing call validation on those devices when you accept their latest software update, you don’t have to wait. You can download the AT&T Call Protect app, or turn on the service from your account settings in myAT&T.
- AT&T Phone digital home phone users can opt-in to get AT&T Digital Phone Call Protect and call validation. Just go to your account settings on myAT&T and turn it on.
- Validation displays will be added to more mobile devices in the new year.
- Finally, a “valid number” display helps fight against bad guys, but it can never guarantee an individual caller is a good guy. Consumers should always use their best judgement when answering calls from strangers.

See also RQ-ATT0000012-RQ-ATT0000023 (<https://sustainability.att.com/priority-topics/network-data-security>).

Within the Accused Instrumentalities, the verification service provider comprises one or more processors, including the processor(s) that operate to perform one or more of the functions described

below. *See, e.g.*, RQ0002113-RQ0002120

(<https://transnexus.com/whitepapers/understanding-stir-shaken/>);
RQ-ATT0000035-RQ-ATT0000041 (<https://www.att.com/security/>).



See, e.g., RQ0002113-RQ0002120 (<https://transnexus.com/whitepapers/understanding-stir-shaken/>).

As another example, the Accused Instrumentalities are implemented, used, and/or put into service by AT&T within its network and in cross-network communications. *See, e.g.*, RQ-ATT0000051-RQ-ATT0000053 (https://about.att.com/story/2019/att_tmo_call-authentication.html).

AT&T* and T-Mobile today began rollout of cross-network call authentication based on SHAKEN/STIR standards – another big step toward protecting consumers from unwanted robocalls.

SHAKEN/STIR technology lets consumers know that an incoming call is really coming from the number listed on the caller ID display – not a spoofed robocall or scammer. While authentication won’t solve the problem of unwanted robocalls by itself, it is a key step toward giving customers greater confidence and control over the calls they answer.

For example, a call that is illegally “spoofed” – or shows a faked number – will fail the SHAKEN/STIR Caller ID verification and will not be marked as verified. By contrast, verification will confirm that a call is really coming from the identified number or entity. More calls will be verified over time as more device providers participate, and as more network providers implement the standards.

The FCC has recommended SHAKEN/STIR standards to digitally validate phone calls. The acronym stands for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR).

For more information on all the ways AT&T is protecting customers, visit https://about.att.com/story/2019/att_call_protect.html and <https://att.com/CyberAware>.

Caller identification authentication and verification technology, including without limitation AT&T's Robocall Mitigation system(s), Call Protect system(s) and service(s), ActiveArmor, the ActiveArmor mobile application, and STIR/SHAKEN, is technology configured to and/or used to, among other functions, detect spoofed phone calls. *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (<https://www.att.com/security/>); RQ0001970 (<https://sti-ga.atis.org/resources/>).

ATIS STANDARD

ATIS-1000074-E -- SIP Forum TWG-10-E

ATIS Standard on –

Signature-based Handling of Asserted information using toKENs (SHAKEN)

1 Scope & Purpose

1.1 Scope

This document is intended to provide telephone service providers with a framework and guidance on how to utilize Secure Telephone Identity (STI) technologies toward the validation of legitimate calls and the mitigation of illegitimate spoofing of telephone identities on IP-based service provider voice networks (also to be referred to as Voice over Internet Protocol [VoIP] networks). The primary focus of this document is on the format of STI claims, the mapping of these claims to SIP (RFC 3261), and the authentication and verification functions.

1.2 Purpose

Using the protocols defined in ~~draft-ietf-stir-rfc4474bis~~ RFC 8224 and ~~draft-ietf-stir-passport~~ RFC 8225, this document defines the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework. This framework is targeted at telephone service providers delivering phone calls over VoIP, and addresses the implementation and usage of the IETF STIR Working Group protocols and the architecture and use of STI-related X.509-based certificates (RFC 5280). It also discusses the general architecture of service provider authentication and verification services. Finally, it provides high level guidance on the use of positive or negative verification of the signature to mitigate illegitimate telephone identity in general.

Illegitimate Caller ID spoofing is a growing concern for North American telephone service providers and their customers. There are many Caller ID spoofing mechanisms, and illegitimate spoofing can evolve to evade mitigation techniques. Service provider solutions must therefore be flexible to respond to evolving threats in much the same way as cybersecurity solutions. In addition, the integration of new technologies into established VoIP networks imposes many interoperability and interworking challenges. As a result, this document is a baseline document on the implementation of the protocol-related requirements for STI. The objective is to provide a baseline that can evolve over time, incorporating more comprehensive functionality and a broader scope in a backward compatible and forward looking manner.

1[b] receive information pertaining to a call initiated by a calling device, the information pertaining to the call including: (1) a value generated based at least in part on information associated with the calling device, and (2) a score generated for the calling device, the score indicating a validity of a phone number;	Within the Accused Instrumentalities, the one or more processors receive or are configured to receive information pertaining to a call initiated by a calling device, the information pertaining to the call including: (1) a value generated based at least in part on information associated with the calling device, and (2) a score generated for the calling device, the score indicating a validity of a phone number. For example, the value generated based at least in part on information associated with the calling device can include a device fingerprint, device information (e.g., make, model, serial number, operating system version, application information, or other identifying information of a device), customer account information, location information, caller or callee number, or other information associated with the device and upon which (or upon verification of which) a security determination is in part based. The value generated based at least in part on information associated with the calling device may be generated from Defendants, a third party (e.g., Hiya), or some combination thereof. For example, the score, which is generated for the calling device, indicates a validity of the phone number and is used to convey assurance or failure to confirm to the callee associated with the call. The received information pertaining to the call includes a score generated for the calling device, the score indicating a validity of a phone number. The score generated for the calling device may be scored from Defendants, a third party (e.g. Hiya), or some combination thereof. The score can be generated by one or more machine learning algorithms. <i>See e.g.</i>, https://work.hiya.com/adaptive-ai-ebook
--	--

Adaptive AI: A Proactive Strategy for Stopping Scam and Fraud Calls

Adaptive AI is an innovative new feature of Hiya Protect, a proprietary call protection service used by carriers, distribution partners and the Hiya mobile app.

Unlike other capabilities on the market today, Adaptive AI uses machine learning to proactively hunt and shut down scam campaigns. With the ability to stay ahead of scammers, Adaptive AI works in real-time, without the need for human intervention or any updating of existing AI models.

See ATT-RQ_0000042, -43, -44 (evidencing device specific data, device settings, installed applications e.g., ActiveArmor, system or application software versions (e.g., “Device OS”, “ActiveArmor Version Information”), contact list data (TN from Device Address Book), or other data associated with the calling device is stored and shared with AT&T’s “Vendor/Partner Hiya”). These values are used to generate a score to indicate a validity of a phone number. That score is used in the process of conveying assurance or failure to confirm for intra- and inter- network calls.

	Active Armor Data Elements As part of the Active Armor Robocall mitigation program, data elements related to calling are shared with our Vendor/Partner Hiya. Note that Hiya’s usage and management of these data elements is under written agreement with AT&T. AT&T GFMO (Global Fraud Management Office) and AT&T CDO (Chief Data Office) each provide a set of per-Number data elements. AT&T CTS/PRS uses an API to provide per-Call data elements. There are additional data elements that are under investigation to determine if they will have value in Robocall Mitigation. The following is a listing of each data element, by data source. See attached spreadsheet for more details.
--	---

AT&T CTS/PRS**Call Direction Response API (Per Call Basis)**

callEventNotification
notificationType
eventDescription
correlationId
callingParticipant
callingParticipantName
callingParticipantAlternate
calledParticipant
callingParticipantPrivacy
callSessionIdentifier
addressDirection:
originatorTasId:
callingParticipantAccessNetworkInfo
callbackData
link

action
actionToPerform
displayName
routingAddress
decisionId
displayAddress
callInfo

	These are additional Parameters Call Direction Response API (CR 245) callInfoLocation callInfoPurpose callInfoType callInfoConfidence callInfoSource callInfoOrigin AT&T Account Services CTN (including AT&T/FN/Cricket customers) Service tier (like Basic vs. Advanced) Service Tags: • FirstNet • CRU • COU • Customers who have rate-plan-included Advanced service. • Cricket • Prepaid • Wireless Home Phone ActiveArmor Application Data TN from Device Address Book - Hashed (shared only with explicit subscriber consent) Device OS ActiveArmor Version Information
--	---

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

	The value generated based at least in part on information associated with the calling device may be generated from Defendants, a third party (e.g., Hiya), or some combination thereof. For example, Enterprise Caller Scoring is a score generated for the calling device that indicates the validity of a phone number. <i>See, e.g., Enterprise Caller Scoring - Stop spammers no matter what phone numbers they use</i>, Hiya Protect, RQ-ATT0000286-RQ-ATT0000291 (https://www.hiya.com/products/enterprise-caller-scoring):
--	---

How it Works

Enterprise Caller Scoring is a new layer of Hiya's Adaptive AI that stops number rotation — the practice of switching phone numbers to avoid spam detection — from being effective on mobile networks.

Like a credit agency for enterprise callers, Enterprise Caller Scoring assesses incoming calls based on the calling enterprise's history across all the numbers they own. It can identify the calling enterprise's reputation for more than 150 million enterprise phone numbers in the US — even phone numbers that haven't yet built a calling history. An enterprise's reputation continuously evolves based on behavior and is automatically recognized across all their numbers.

See also Michelle Wallace, *How Hiya's Proprietary Adaptive AI Stops Phone Spam*, Hiya Protect, <https://blog.hiya.com/how-hiyas-proprietary-adaptive-ai-stops-phone-spam>.

Both the value and the score generated for the calling device may be generated by Defendants'

systems, a third party (e.g. Hiya) at Defendant’s request or direction, or some combination thereof. The value and score can be used to detect spoofed, spam and/or fraudulent phone calls.

As another example, the Accused Instrumentalities receive and/or are configured to receive information pertaining to a call initiated by a calling device. *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (<https://www.att.com/security/>); RQ-ATT0000012-RQ-ATT0000023 (<https://sustainability.att.com/priority-topics/network-data-security>). For example, STIR/SHAKEN comprises a verification service provider (STI-VS). *See, e.g.*, RQ0001970 (<https://sti-ga.atis.org/resources/>):

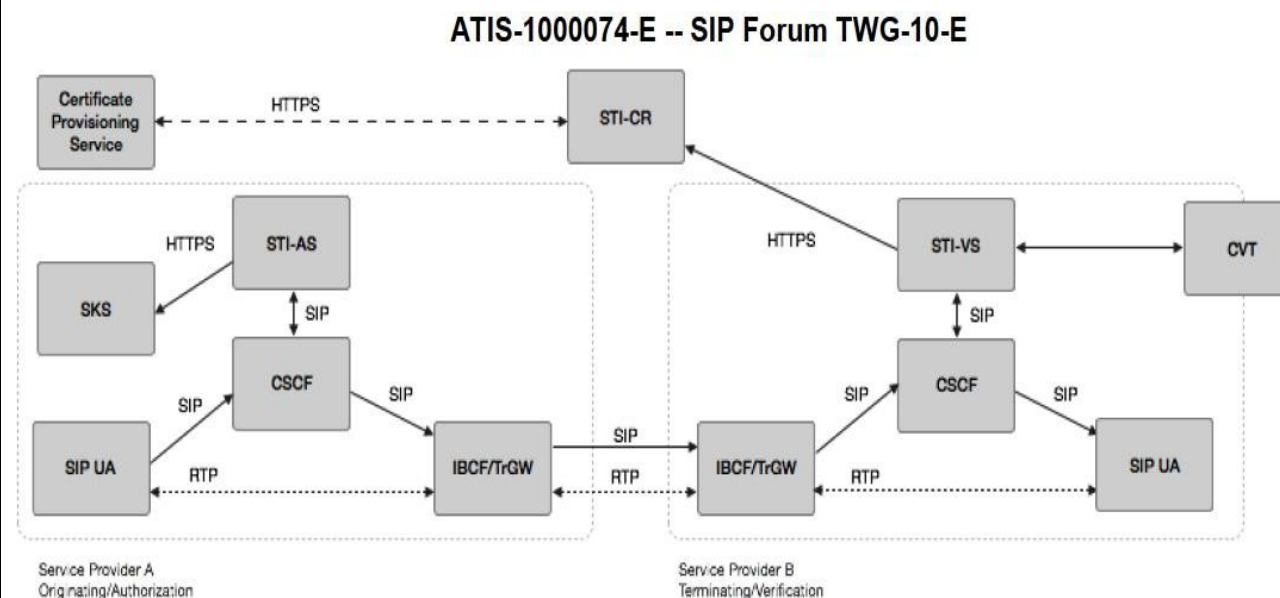


Figure 4.1 – SHAKEN Reference Architecture

	This SHAKEN reference architecture includes the following elements: • SIP UA – The SIP User Agent authenticated by the service provider network. When the SIP UA is under direct management control of the telephone service provider, the service provider network can assert the calling party identity in originating SIP INVITE requests initiated by the SIP UA. • IMS/Call Session Control Function (CSCF) – This component represents the SIP registrar and routing function. It also has a SIP application server interface. • Interconnection Border Control Function (IBCF)/Transition Gateway (TrGW) – This function is at the edge of the service provider network and represents the Network-to-Network Interface (NNI) or peering interconnection point between telephone service providers. It is the ingress and egress point for SIP calls between providers. • Authentication Service (STI-AS) – The SIP application server that performs the function of the authentication service defined in ~~draft-ietf-stir-rfc4474bis~~RFC 8224. It should either itself be highly secured and contain the Secure Key Store (SKS) of secret private key(s) or have an authenticated, Transport Layer Security (TLS)-encrypted interface to the SKS that stores the secret private key(s) used to create PASSporT signatures. • Verification Service (STI-VS) – The SIP application server that performs the function of the verification service defined in ~~draft-ietf-stir-rfc4474bis~~RFC 8224. It has an Hypertext Transfer Protocol Secure (HTTPS) interface to the Secure Telephone Identity Certificate Repository that is referenced in the Identity header field to retrieve the provider public key certificate. • Call Validation Treatment (CVT) – This is a logical function that could be an application server function or a third party application for applying anti-spoofing mitigation techniques once the signature is positively or negatively verified. The CVT can also provide information in its response that indicates how the results of the verification should be displayed to the called user. • SKS – The Secure Key Store is a logical highly secure element that stores secret private key(s) for the authentication service (STI-AS) to access. • Certificate Provisioning Service – A logical service used to provision certificate(s) used for STI. • Secure Telephone Identity Certificate Repository (STI-CR) – This represents the publically accessible store for public key certificates. This should be an HTTPS web service that can be validated back to the owner of the public key certificate. As one example, within the Accused Instrumentalities, the received information pertaining to the call includes a value generated based at least in part on information associated with the calling device. For example, the SIP Identity header is generated from information associated with the device. <i>See, e.g.</i>, RQ0001970 (https://sti-ga.atis.org/resources/). As one example, the SIP Identity header comprises the Personal Assertion Token (PASSporT), which is a value generated based at least in part on information associated with the calling device. <i>See, e.g.</i>, RQ0001970 (https://sti-
--	--

ga.atis.org/resources/).

4.1 STIR Overview

The documents ~~-ietf-stir-rfc4474bis~~[RFC 8224](#) and ~~ietf-stir-passport~~[RFC 8225](#) define a set of protocol level tools that can be used in Session Initiation Protocol (SIP) for applying digital signatures to the Caller ID or telephone number of the calling party.

4.1.1 Personal Assertion Token (PASSporT) Token

The document ~~-ietf-stir-passport~~[RFC 8225](#) defines a token-based signature that combines the use of JavaScript Object Notation (JSON) Web Tokens, JSON Web Signatures, and X.509 certificate key pairs, or Public Key Infrastructure (PKI), to create a trusted signature. The authorized owner of the certificate used to generate the signature can be validated and traced back to the known trust anchor who signed the certificate. The Personal Assertion Token (PASSporT) ~~token~~ includes a number of claims the signer of the token is asserting. The associated public certificate is used to verify the digital signature and the claims included in the PASSporT~~token~~. The public certificate is also used to validate the entity that signed the token through a Service Provider Identifier (SPID), as defined in ~~ietf-stir-certificates~~[RFC 8226](#). The validated claims and the validated identity of the entity signing the claims can both be used to determine the level of trust in the originating entity and their asserted calling party information. Call blocking applications or other mitigation techniques could use the information over time to determine "reputation" of the entity signing the token, which could provide further input to determine the level of trust for the calling party information. Note that PASSporTs~~tokens~~ and signatures themselves are agnostic to network signaling protocols but are used in ~~draft-ietf-stir-rfc4474bis~~[RFC 8224](#) to define specific SIP usage as described in the next section.

See also J. Peterson et al., *Authenticated Identity Management in the Session Initiation Protocol (SIP)*, Internet Engineering Task Force (Feb. 2018), RQ0001971-RQ0002016 (<https://tools.ietf.org/html/rfc8224>).

Step 4: Populate and Add the Identity Header

Subsequently, the authentication service MUST form a PASSporT object and add a corresponding Identity header field to the request containing either the full or compact form of PASSporT. For the baseline PASSporT header (headers containing no "ppt" parameter), this follows the procedures in [Section 4](#); if the authentication service is using an alternative "ppt" format, it MUST add an appropriate "ppt" parameter and follow the procedures associated with that extension (see [Section 9](#)). After the Identity header field has been added to the request, the authentication service MUST also add an "info" parameter to the Identity header field. The "info" parameter contains a URI from which the authentication service's credential can be acquired; see [Section 7.3](#) for more on credential acquisition.

6.2. Verifier Behavior

This document specifies a logical role for SIP entities; this role is called a verification service, or verifier. When a verifier receives a SIP message containing one or more Identity header fields, it inspects the signature(s) to verify the identity of the originator of the message. The results of a verification are provided as input to an authorization process that is outside the scope of this document.

See also C. Wendt & J. Peterson, *PASSport: Personal Assertion Token*, Internet Engineering Task Force (Feb. 2018), RQ0002017-RQ0002041 (<https://datatracker.ietf.org/doc/html/rfc8225>).

PASSport specifically uses this token format and defines claims that convey the identity of the origination and destination of personal communications. The primary value asserted in a PASSport object is the originating identity representing the identity of the calling party or the initiator of a personal-communications session. The signer of a PASSport object may or may not correspond to the originating identity. For a given application's use or using protocol of PASSport, the creation of the PASSport object is performed by an entity that is authoritative to assert the caller's identity. This authority is represented by the certificate credentials and the signature, and the PASSport object is created and initiated to the destination(s) per the application's choice of authoritative point(s) in the network. For example, the PASSport object could be created at a device that has authenticated with a user or at a network entity with an authenticated trust relationship with that device and its user. Destination identities represent the intended destination of the personal communications, i.e., the identity(s) being called by the caller. The destination point or points determined by the application need to have the capability to verify the PASSport and the digital signature. The PASSport-associated certificate is used to validate the authority of the originating signer, generally via a certificate chain to the trust anchor for that application.

Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP)

Alliance for Telecommunications Industry Solutions

Approved October 2015

Abstract

This specification defines best practices for obtaining the device identifiers (e.g., International Mobile Equipment Identity [IMEI]) from mobile devices even if the mobile device is locked or disabled. This best practices specification was developed in response to Recommendation 1.5 of the December 4, 2014 Federal Communications Commission (FCC) Technological Advisory Council (TAC) report on Mobile Device Theft Prevention (MDTP).

5.2.4 Origination Identifier (“origid”)

In addition to attestation, the unique origination identifier (“origid”) is defined as part of SHAKEN. This unique origination identifier should be a globally unique string corresponding to a Universally Unique Identifier (UUID) (RFC 4122).

The purpose of the unique origination identifier is to assign an opaque identifier corresponding to all or part of the originating service provider’s network (data centers, IBCF nodes, access networks, IMS core complexes, etc.) ~~initiated calls themselves~~, customers, customer or interconnecting service provider nodes, classes of customer devices, or other groupings that a service provider might want to use to indicate common call sources for determining things such as reputation or trace back identification of customers or gateways.

The origid is not intended to directly expose or be reverse-engineered to a customer or service provider identity, but it should be useful for analytics purposes in remote networks and traceback within the originating service provider network.

Best practices will specify when it is appropriate to use groupings less-granular than per-customer, customer device or node, or interconnecting service provider or interconnecting service provider node for origination identifier marking. Where origination identifier granularity is at the customer level or finer, best practices should also cover methods to protect the privacy of individual customers whose identity might be deduced through calling patterns. ~~For Full Attestation, in general, a single identifier will be used as part of the certificate representing direct service provider initiated calls on its VoIP network. A service provider may, for example, also choose to have a pool of identifiers to differentiate geographic regions or classes of customers. Best practices will likely develop as trace back and illegitimate call identification practices evolve.~~

~~For Partial Attestation, a single identifier per customer is required in order to differentiate calls both for trace back and reputation segmentation so that one customer’s reputation doesn’t affect other customer’s or the service provider’s call reputation. A service provider may choose to be more granular (e.g., per node per customer) depending on its size and classes of services that the service provider offers.~~

~~For Gateway Attestation, best practices will dictate that the “origid” should be sufficiently granular to identify the originating node or trunk to allow for trace back identification and reputation scoring.~~

AT&T further discloses that the Accused Instrumentalities receive and use the following information associated with the calling device. *See, e.g., AT&T Privacy Notice*, AT&T, RQ-ATT0000070-RQ-ATT0000086 (<https://about.att.com/privacy/privacy-notice.html>):

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

	The information we collect x To better run our business, we collect information about you, your equipment and how you use our products and services. This can include: • Account information. You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including Customer Proprietary Network Information. • Equipment information. We collect information about equipment on our network like the type of device you use, device ID, and phone number. • Network performance. We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working. • Location information. Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites. • Web browsing and app information. We automatically collect a variety of information which may include time spent on websites or apps, website and IP addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information. • Biometric information. Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our Biometric Information Privacy Notice. • Third-party information. We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T.
--	--

	How we use your information x We rely on the information we collect to support our business functions, power our services and improve your experience, such as when we: • Combine it with the information from testing and running our network to determine which products and services better meet the needs of our customers. • Provide our products and services. • Contact you. • Improve your experience and safety. This includes verifying your identity, detecting and preventing fraud, protecting your financial accounts, authorizing transactions and assisting your interactions with customer care. • Improve and protect our network. • Use it to help understand which additional products and services may interest you and others. (We don’t access or use the content of your texts, emails or calls for this or any other marketing and advertising.) • Design and deliver advertising, marketing and promotional campaigns to you and others – and measuring their effectiveness (See your choices). • Use it for billing, collection, and protection of our property and legal rights. • Prevent and investigate security issues, illegal activities, and violations of our terms and conditions. • Conduct research and create aggregated reports – reports that offer insights about groups of customers, but not individuals (we do not attempt to re-identify individuals in aggregated reports). <i>See also AT&T ActiveArmor Mobile Security Application and Service, AT&T, RQ-ATT0000139-RQ-ATT0000150 (https://www.att.com/legal/terms.activeArmorMobileSecurity.html):</i>
--	---

	In order to perform the functions of the Service including but not limited to its Call Features, AT&T may use and/or disclose or allow the disclosure to our third-party vendor(s) of Your personal information, including without limitation mobile number, contacts/address book in order to populate detail in the call detail screen, the presence or absence of calling party phone numbers in your Device address book, and App usage information, such as which numbers you report and/or manually block within the App, as factors to determine which callers are suspected fraud and spam. The contact names and phone numbers in your Device address book are not shared for any purpose other than improving your experience with the App by helping you to recognize known callers. 3.2 Consent for Information Disclosure in Connection with Data Features The Service includes the following data security and related features: Device Security Alerts, Data Breach Alerts, Public Wi-Fi Protection (VPN & Wi-Fi Alerts), Identity Monitoring, Reverse Number Lookup, Safe Browsing, and Device Theft Alerts (collectively “Data Features”) In order to perform the functions and to improve the effectiveness of the Service including but not limited to its Data Features for all users, AT&T, its pertinent suppliers and their subsidiaries, agents and subcontractors may collect, maintain, process, use, and disclose diagnostic, technical, usage and related information including, but not limited to, information about: • the type of Device You are using and the operating system You are running; • Your applicable wireless network provider/carrier; • the applications and files present on Your Device and SD memory card; • the results of any scans performed by the App; and • actions You take as a result of any virus or malware notifications. We also may collect information about how the App and any associated Service applications behave on Your Device and the network services with which applications installed on Your Device communicate in order to determine if any applications are behaving maliciously (for example, is an application accessing Your address contacts, sending premium-rate text messages that charge money to Your wireless bill, or communicating with a server known to host phishing websites). As one example, within the Accused Instrumentalities, the received information pertaining to the call includes a score generated for the calling device, the score indicating a validity of a phone number. For example, the score generated for the calling device comprises and/or has as an input or signal, among other inputs and/or signals, an indication of the attestation level associated with the calling device and indicates a validity of a phone number, but the score is not limited to the A or B or C attestation level. <i>See, e.g.</i>, RQ0001970 (https://sti-ga.atis.org/resources/).
--	---

5.2.3 Attestation Indicator (“attest”)

The “attest” claim allows the originating service provider that is populating an Identity header to clearly indicate the information it can vouch for regarding the origination of the call.

~~This indicator allows for both identifying the service provider that is vouching for the call as well as clearly indicating what information the service provider is attesting to.~~

In the SHAKEN framework we define the following three levels of attestation:

A. Full Attestation: The signing provider shall satisfy all of the following conditions:

- Is responsible for the origination of the call onto the IP-based service provider voice network.
- Has a direct authenticated relationship with the customer and can identify the customer.
- Has established a verified association with the telephone number used for the call.

NOTE 1: The signing provider is asserting that their customer can “legitimately” use the number that appears as the calling party (i.e., the Caller ID). The legitimacy of the telephone number(s) the originator of the call can use is subject to signer-specific policy, but could use mechanisms such as the following:

- The number was assigned to this customer by the signing service provider.
- This number is one of a range of numbers assigned to an enterprise or wholesale customer.
- The signing service provider has ascertained that the customer is authorized to use a number (e.g., by business agreement or evidence the customer has access to use the number). This includes numbers assigned by another service provider.
- The number is not permanently assigned to an individual customer but the signing provider can track the use of the number by a customer for certain calls or during a certain timeframe.

NOTE 2: Ultimately it is up to service provider policy to decide what constitutes “legitimate right to assert a telephone number” but the service provider’s reputation may be directly dependent on how rigorous they have been in making this assertion.

B. Partial Attestation: The signing provider shall satisfy all of the following conditions:

- Is responsible for the origination of the call onto ~~its~~ the IP-based service provider voice network.
- Has a direct authenticated relationship with the customer and can identify the customer.
- Has NOT established a verified association with the telephone number being used for the call.

9

ATIS-1000074-E -- SIP Forum TWG-10-E

NOTE: By populating this value, the service provider attests that it can trace the source of the call to a customer for policy enforcement purposes~~When partial attestation is used, each customer will have a unique origination identifier created and managed by the service provider, but the intention is that it will not be possible to reverse engineer the identity of the customer purely from the identifier or signature. As described in section 5.2.4, the unique origination identifier allows data analytics to establish a reputation profile and assess the reliability of information asserted by the customer assigned this unique identifier. The identifier also provides a reliable mechanism to determine the customer for forensic analysis or legal action where appropriate.~~

The verifier validates that the PASSporT ~~token~~ provided in the Identity header of the INVITE includes all of the baseline claims, as well as the SHAKEN extension claims. The verifier shall also follow the ~~draft-ietf-stir-#64474bis~~ RFC 8224-defined verification procedures to check the corresponding date, originating identity (i.e., the originating telephone number) and destination identities (i.e., the terminating telephone numbers), with the restrictions specified in this section.

	C. Gateway Attestation: The signing provider shall satisfy all of the following conditions: ~~• Is the entry point of the call into its VoIP network.~~ • Has no relationship with the initiator of the call (e.g., international gateways). ~~NOTE: The token will provide a unique origination identifier of the node in the “origid” claim. (The signer is not asserting anything other than “this is the point where the call entered my network”.)~~ <u>NOTE: The signer/originating service provider should be able to trace a call to an interconnecting service provider and/or peer node for traceback or policy enforcement purposes. Gateway attestation may also be used when the STI-AS does not have sufficient information for determining that A or B attestation applies even when the call was received at a customer interface.</u> For the PASSporT extension claim, the “attest” key value pair shall be set to uppercase characters “A”, “B”, or “C” corresponding to the appropriate attestation defined above. An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
1[c] perform a security determination based at least in part on the score generated for the calling device, and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device; and	Within the Accused Instrumentalities, the one or more processors perform and/or are configured to perform a security determination based at least in part on the score generated for the calling device, and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device. The Accused Instrumentalities perform and/or are capable of performing a security determination based at least in part on the score generated for the calling device and at least in part by verifying the value included in the information pertaining to the call, from Defendants, a third party (e.g. Hiya), or some combination thereof. <i>See e.g., https://work.hiya.com/adaptive-ai-ebook</i>

Adaptive AI: A Proactive Strategy for Stopping Scam and Fraud Calls

Adaptive AI is an innovative new feature of Hiya Protect, a proprietary call protection service used by carriers, distribution partners and the Hiya mobile app.

Unlike other capabilities on the market today, Adaptive AI uses machine learning to proactively hunt and shut down scam campaigns. With the ability to stay ahead of scammers, Adaptive AI works in real-time, without the need for human intervention or any updating of existing AI models.

For example, the value generated based at least in part on information associated with the calling device can include a device fingerprint, device information (e.g., make, model, serial number, operating system version, application information, or other identifying information of a device), customer account information, location information, caller or callee number, or other information associated with the device and upon which (or upon verification of which) a security determination is in part based. The value generated based at least in part on information associated with the calling device may be generated from Defendants, a third party (e.g., Hiya), or some combination thereof and is verified as part of the security determination when deciding to connect, convey assurance of the callee, convey a failure to confirm the callee, and/or refuse to connect the initiated call. For example, Defendant's Robocall mitigation system performs a security determination based at least in part on the score generated for the calling device, and at least in part by verifying the value. *See* ATT-RQ_0000042, -43, -44 (evidencing device specific data, device settings, installed applications

e.g., ActiveArmor, system or application software versions (e.g., “Device OS”, “ActiveArmor Version Information”), contact list data (TN from Device Address Book), or other data associated with the calling device is stored and shared with AT&T’s “Vendor/Partner Hiya”). These values are used, along with one or more scores to determine the validity of a phone number. Furthermore, the score and value are used in the process of conveying assurance or failure to confirm for intra- and inter- network calls.

Active Armor Data Elements

As part of the Active Armor Robocall mitigation program, data elements related to calling are shared with our Vendor/Partner Hiya. Note that Hiya’s usage and management of these data elements is under written agreement with AT&T.

AT&T GFMO (Global Fraud Management Office) and AT&T CDO (Chief Data Office) each provide a set of per-Number data elements. AT&T CTS/PRS uses an API to provide per-Call data elements. There are additional data elements that are under investigation to determine if they will have value in Robocall Mitigation.

The following is a listing of each data element, by data source. See attached spreadsheet for more details.

AT&T CTS/PRS**Call Direction Response API (Per Call Basis)**

callEventNotification
 notificationType
 eventDescription
 correlationId
 callingParticipant
 callingParticipantName
 callingParticipantAlternate
 calledParticipant
 callingParticipantPrivacy
 callSessionIdentifier
 addressDirection:
 originatorTasId:
 callingParticipantAccessNetworkInfo
 callbackData
 link

 action
 actionToPerform
 displayName
 routingAddress
 decisionId
 displayAddress
 callInfo

These are additional Parameters Call Direction Response API (CR 245)

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

CTN (including AT&T/FN/Cricket customers)

Service tier (like Basic vs. Advanced)

Service Tags:

- FirstNet
- CRU
- COU
- Customers who have rate-plan-included Advanced service.
- Cricket
- Prepaid
- Wireless Home Phone

ActiveArmor Application Data

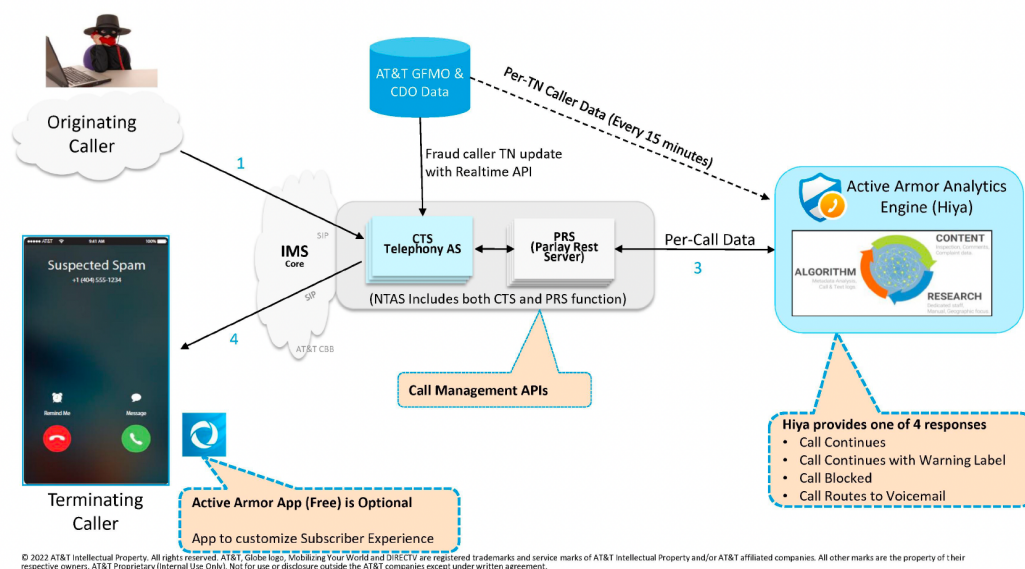
TN from Device Address Book - Hashed (shared only with explicit subscriber consent)

Device OS

ActiveArmor Version Information

See, e.g., ATT-RQ_0000045 showing that Hiya provides at least one of 4 responses – namely, “Call Continues,” “Call Continues with Warning Label”, “Call Blocked” or “Call Routes to Voicemail” (e.g., whether or not the call should be connected or blocked).

AT&T Active Armor (Call Protect) – High Level Architecture



© 2022 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T companies except under written agreement.

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

ATT-RQ_0000045

As another example, Enterprise Caller Scoring is a score generated for the calling device that indicates the validity of a phone number. *See, e.g., Enterprise Caller Scoring - Stop spammers no matter what phone numbers they use, Hiya Protect, RQ-ATT0000286-RQ-ATT0000291* (<https://www.hiya.com/products/enterprise-caller-scoring>):

How it Works

Enterprise Caller Scoring is a new layer of Hiya's Adaptive AI that stops number rotation — the practice of switching phone numbers to avoid spam detection — from being effective on mobile networks.

Like a credit agency for enterprise callers, Enterprise Caller Scoring assesses incoming calls based on the calling enterprise's history across all the numbers they own. It can identify the calling enterprise's reputation for more than 150 million enterprise phone numbers in the US — even phone numbers that haven't yet built a calling history. An enterprise's reputation continuously evolves based on behavior and is automatically recognized across all their numbers.

See also <https://blog.hiya.com/how-hiyas-proprietary-adaptive-ai-stops-phone-spam>.

As another example, the Accused Instrumentalities perform and/or are capable of performing a security determination based at least in part on the SIP Identity header. The SIP Identity header is

	based at least in part on the score generated for the calling device, and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device. <i>See, e.g.</i>, RQ0001970 (https://sti-ga.atis.org/resources/). As one example, the Accused Instrumentalities perform and/or are capable of performing a security determination based at least in part on a public certificate, which is verifying the value comprised in the SIP Identity header included in the information pertaining to the call initiated by the calling device. As one example, the value is the Personal Assertion Token (PASSporT). [The verifier validates that the PASSporT ~~token~~ provided in the Identity header of the INVITE includes all of the baseline claims, as well as the SHAKEN extension claims. The verifier shall also follow the ~~draft-ietf-stir-fc4474bis~~<u>RFC 8224</u>-defined verification procedures to check the corresponding date, originating identity (i.e., the originating telephone number) and destination identities (i.e., the terminating telephone numbers), <u>with the restrictions specified in this section</u>. As one example, the Accused Instrumentalities perform or are capable of performing a security determination based at least in part on the attestation level. The attestation level is based at least in part on the score generated for the calling device and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device. <i>See, e.g.</i>, RQ0001970 (https://sti-ga.atis.org/resources/).
--	--

Use of standardized cryptographic digital signatures to validate the originator of a signed identity can provide a verifiable mechanism to identify the authorized originator of a call into the VoIP network with non-repudiation. Further, the use of an assigned attestation indicator and a unique origination identifier depending on how and where the call is originated in the VoIP network represents the originating signer’s ability to vouch for the accuracy of the source of origin of the call. For example, if the service provider has an authenticated direct relationship with the origination of the call, this attestation is categorized differently than calls that are originated from different networks or gateways that the service provider may have received from an unauthenticated network or that are

3

ATIS-1000074-E -- SIP Forum TWG-10-E

unsigned. Verifiers of signatures will use these attestations as information to provide trace back mechanisms, as well as information to feed into any call spam identification solution enabled on behalf of their customer.

5.2.2 PASSporT Extension “shaken”

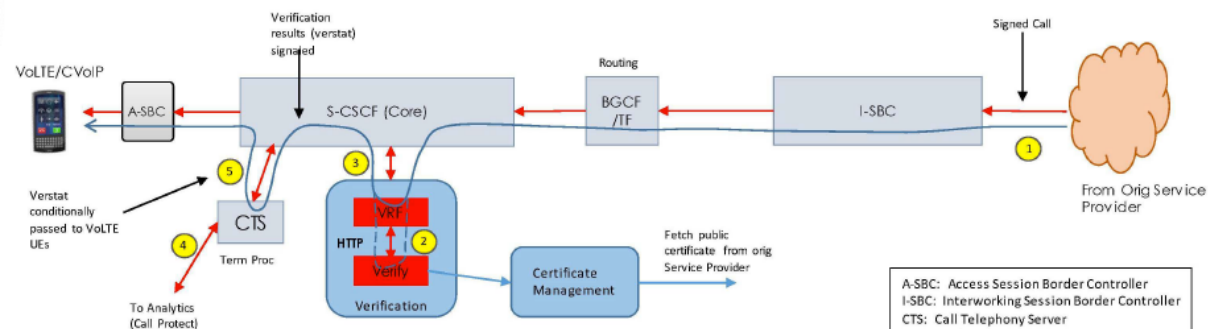
The base PASSporT set of claims cover the assertion of the originating telephone number along with date and destination telephone numbers to avoid replay attacks using valid Identity header fields. draft-ietf-stir-passport-shaken defines ~~This section will detail a specific~~ the “shaken” extension to ~~the~~ PASSporT to cover the following requirements of SHAKEN. The ~~SHAKEN~~ “shaken” extension to PASSporT shall be implemented with all extension claims as part of the signed PASSporT ~~token~~.

1. The ability to provide an attestation indicator for the context of how the call was originated.
2. The ability to provide a unique originating identifier, as described in Section 5.2.4, that can serve as an opaque indication of where in the originating service provider’s network the call was originated. ~~This identifier shall be globally unique and consistent so it can be used in analytics for tracking the reputation of a particular originating service and could also be used for any traceback efforts if a particular originator is a consistent or pervasive “bad actor”.~~

The PASSporT “shaken” extension shall include both an attestation indicator (“attest”), as described in section 5.2.3 and an origination identifier (“origid”) as described in section 5.2.4. The SHAKEN PASSporT ~~token~~ would have the form given in the example below:

As another example, intra-network calls may be treated differently from inter-network calls. The attestation level of a call may be included within a verstat (verification indicator) tag, or other header. See e.g., ATT-RQ-466, 467.

Inter-Network SHAKEN Flows (ATT terminated)



1. Signed call is received from an originating carrier that supports SHAKEN. Terminating S-CSCF detects the received identity header and sends the call to the VRF.
2. The VRF formulates the HTTP verification request and sends the request to the Verification Server.
3. The verification results are returned and signaled in the "verstat" parameter (contained in PAI/From headers).
4. Verstat is used by analytics (e.g. Call Protect) as an input to reputation scoring.
5. Verstat is conditionally passed to terminating VoLTE UE and UE uses this information to influence the calling number/name display information. For CVoIP, term CTS modifies the Calling Number to include SHAKEN verification results.

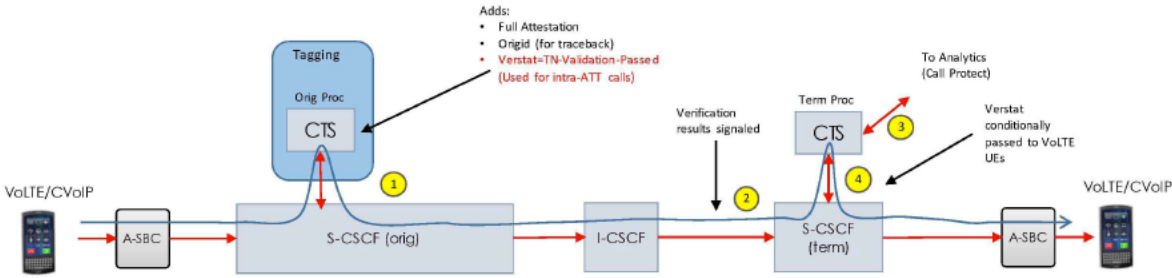
AT&T Proprietary and Confidential

This document and information contained therein is not for use or disclosure outside of AT&T

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

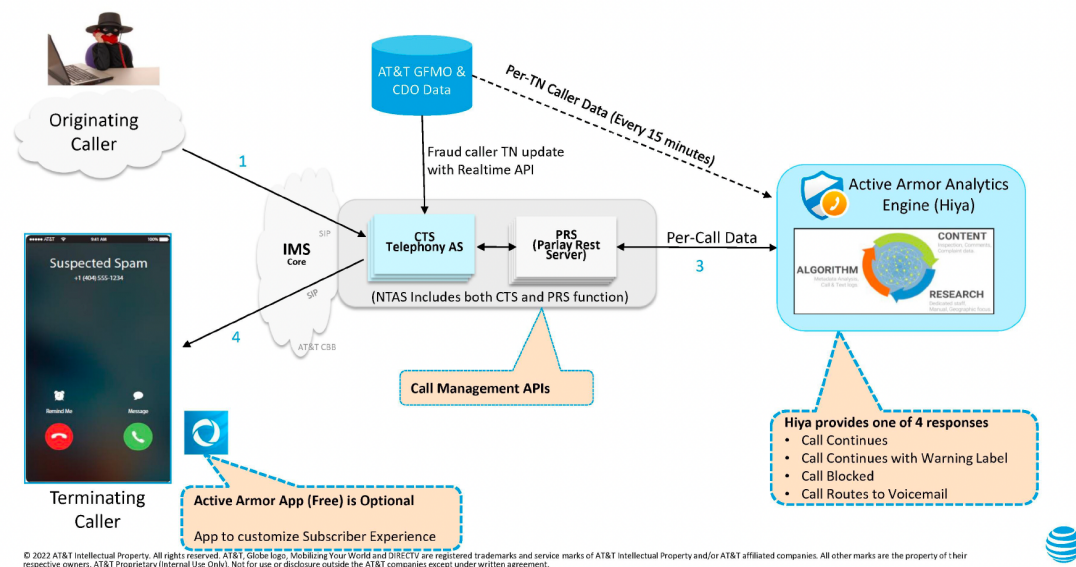


ATT-RQ_0000466

	Intra-AT&T SHAKEN Flows  The diagram illustrates the Intra-AT&T SHAKEN Flows. It shows a call path starting from a VoLTE/CVoIP device, passing through an A-SBC, then an S-CSCF (orig), then an I-CSCF, then an S-CSCF (term), and finally through another A-SBC to a terminating VoLTE/CVoIP device. Key components include the Tagging process (adding Orig Proc and CTS) and the Term Proc (CTS). Verification results are signaled from the I-CSCF to the S-CSCF (term). Analytics (Call Protect) receive verstat information from the S-CSCF (term) and pass it to the terminating A-SBC. A legend defines the components: A-SBC: Access Session Border Controller, CTS: Call Telephony Server, I-CSCF: Interrogating Call Session Control Function, S-CSCF: Serving Call Session Control Function. - After originating processing is completed, CVoIP/VoLTE calls will be “tagged”. - Tagging adds verstat parameter to emulate a call that was verified successfully. This is used for intra-network (ATT to ATT) calls. - Intra-ATT calls are not “signed” - The emulated verification result (verstat) is passed to CTS. - Verstat is used by analytics (e.g. Call Protect) as an input to reputation scoring. - Verstat is conditionally passed to terminating VoLTE UE and UE uses this information to influence the calling number/name display information. For CVoIP, term CTS modifies the Calling Number to include SHAKEN verification results. ATT-RQ_0000467
1[d] based at least in part on the security determination, perform at least one of conveying an assurance to a callee associated with the call or conveying a failure to confirm to the callee associated with the call; and	Within the Accused Instrumentalities, based at least in part on the security determination, the one or more processors perform and/or are configured to perform at least one of conveying an assurance to a callee associated with the call or conveying a failure to confirm to the callee associated with the call. <i>See, e.g.,</i> ATT-RQ_0000045 showing that Hiya provides at least one of 4 responses – namely, “Call Continues,” “Call Continues with Warning Label”, “Call Blocked” or “Call Routes to Voicemail”

(e.g., indicating whether or not the call should convey an assurance to a callee associated with the call or convey a failure to confirm to the callee).

AT&T Active Armor (Call Protect) – High Level Architecture



RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

ATT-RQ_0000045

As one example, based at least in part on the security determination, the Accused Instrumentalities convey and/or are configured to convey an assurance to a callee associated with the intra- or inter-network call, including but not limited to conveying a green check, “valid number,” or “[V]”, brand logos, contact/caller name, and/or otherwise providing call logs, reports, or other indications reflecting confirmation.

See, e.g., RQ-ATT0000024-RQ-ATT0000026
https://about.att.com/story/2019/call_validation_displays.html):



	<i>Samsung Galaxy S10, Galaxy S10+, LG V40 ThinQ and AT&T Digital Home Phone Service Can Now Show That a Call Is Authenticated</i> AT&T* has turned on its first phone displays that let you know an incoming call is really from the number appearing on Caller ID. This fights against “spoofing” of phone numbers – a trick used by many illegal robocallers. Most AT&T customers with a Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ™ will see a special display when an incoming call has been authenticated. They will see a green checkmark and the words, “Valid Number.” Consumers with AT&T Phone digital home phone service also can activate the feature. It will give them a “[V]” for valid number. Phone service providers have jointly developed a technology – the SHAKEN/STIR standards – to digitally validate calls. This won’t solve the problem of unwanted robocalls by itself. But it can give consumers greater confidence and control over the calls they answer. “This is another step to tame annoying, unwanted robocalls,” said Kevin Petersen, AT&T senior vice president, Postpaid Wireless Products. “In the coming year, we’ll continue to take more steps and put more pressure on the bad guys.” AT&T is rolling out its SHAKEN/STIR display as part of its AT&T Call Protect service, which is being added at no charge to millions of mobility consumer lines. AT&T Call Protect blocks or labels suspected illegal and unwanted robocalls.
--	--

This strategy will give a multiplier effect to call protection: A “valid number” on an AT&T device means the incoming call has been authenticated by SHAKEN/STIR *and* passed through AT&T Call Protect screening.

Here are some other key points:

- A call that shows “valid number” has been verified and can increase your trust level. But a call without the label may still be a legitimate call. More calls will be marked with “valid number” over time, as more network providers implement SHAKEN/STIR and link to each other.
- AT&T has rolled out AT&T Call Protect automatically to many Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ users. Others are on the way soon.¹ If you’re not seeing call validation on those devices when you accept their latest software update, you don’t have to wait. You can download the AT&T Call Protect app, or turn on the service from your account settings in myAT&T.
- AT&T Phone digital home phone users can opt-in to get AT&T Digital Phone Call Protect and call validation. Just go to your account settings on myAT&T and turn it on.
- Validation displays will be added to more mobile devices in the new year.
- Finally, a “valid number” display helps fight against bad guys, but it can never guarantee an individual caller is a good guy. Consumers should always use their best judgement when answering calls from strangers.

See, e.g., RQ-ATT0000137-RQ-ATT0000138 (<https://www.att.com/support/article/u-verse-voice/KM1235421/>):

Digital Phone Call Protect features

Here's what you get with Digital Phone Call Protect¹:

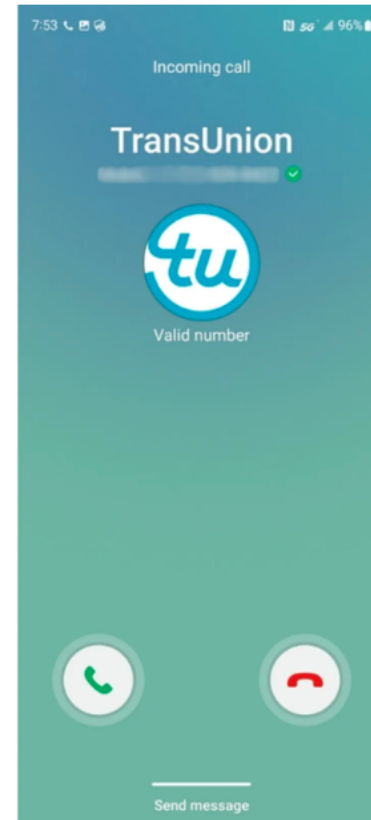
- **Call validation:** Soon you'll see a [V] on your caller ID for some calls. This means we've confirmed that the call originated from the phone registered to that number. (Remember to still be cautious when answering a call from an unknown number.)
- **Automatic fraud blocking:** Each potential fraud call gives the caller a busy signal, and the call won't go through. You can toggle this feature on or off.
- **Call blocking:** If you have a specific number you want to block, press *61 after the unwanted call to block that number.
- **Call log:** You can see detailed call log info.
- **Suspected spam call warning:** Your caller ID will show Suspected Spam and a type (Political, Nonprofit, Telemarketer, Survey, or Robocaller).

See also AT&T Will Warn You of Incoming Robocalls – But Not on iPhone, AT&T, RQ-ATT0000088-RQ-ATT0000090 (<https://www.idropnews.com/news/fast-tech/att-will-warn-you-of-incoming-robocalls-but-not-on-iphone/125657/>):

It's worth noting that AT&T also offers call verification for iPhone users, *but it won't show up when the call is coming in.*

- To see if a number is verified on iPhone, you'll need to check your call log in the **Phone app** under **Recents**.
- Verified unknown calls will have a checkmark next to them on recent versions of iOS. This clunky method is likely to change in the future, however.

See, e.g., AT&T's New Robocall-Fighting Tool Adds Logo Images to Caller ID, CNET, RQ-ATT0000091-RQ-ATT0000094 (<https://www.cnet.com/tech/mobile/at-t-adopts-new-robocall-fighting-tool-that-adds-logo-images-to-caller-id/>):



An example of a company logo that appears when a carrier uses Branded Call Display to authenticate a call.

As another example, based at least in part on the security determination, the Accused Instrumentalities convey and/or are configured to convey a failure to confirm to the callee associated with the inter- or intra- network call, including but not limited by conveying “Unknown caller,” any indication of a potential spoofed, spam, or fraudulent call, such as “suspected spam” or “suspected fraud,” any indication a call was blocked, and/or by with an allowed communication not conveying an assurance such as a green check, “valid number,” or “[V]”, a brand logo, contact/caller name, or providing a call log, report, or other indication reflecting confirmation.

	<i>See, e.g.,</i> RQ-ATT0000095-RQ-ATT0000098 (https://forums.att.com/conversations/account-features/blocking-unknown-numbers/63b33783c1c54d548b8bbe5b). Hey, rehjaeger! The AT&T ActiveArmor application allows you to flag, send to voicemail, and block nuisance & fraud risk calls. You can also send unknown callers to voicemail. To find these settings, you'll open up the AT&T ActiveArmor app then click on the phone icon named Calls. After, you'll scroll down until you see Network Call Preferences. From there, select the drop down arrow listed near Unknown callers and click send to voicemail. Keep in mind, you can only see these settings while connected to your cellular data. To answer your question you can't personally block all unknown callers but you can automatically forward them to your voicemail. We hope we've answered your question! Please let us know if you have additional inquiries! Jonye, AT&T Community Specialist <i>See, e.g., AT&T Text-Blocking Sets a Record</i>, AT&T, RQ-ATT0000046-RQ-ATT0000048 (https://about.att.com/blogs/2023/activearmor-text-blocking.html). • We block all the fraud calls we can find. And we label suspected spam calls so you can choose to answer or not. We do this for every customer on our network – more than a billion blocked or labeled calls a month. <i>See, e.g.,</i> RQ-ATT0000051-RQ-ATT0000053 (https://about.att.com/story/2019/att_tmo_call-authentication.html):
--	---

AT&T* and T-Mobile today began rollout of cross-network call authentication based on SHAKEN/STIR standards – another big step toward protecting consumers from unwanted robocalls.

SHAKEN/STIR technology lets consumers know that an incoming call is really coming from the number listed on the caller ID display – not a spoofed robocall or scammer. While authentication won’t solve the problem of unwanted robocalls by itself, it is a key step toward giving customers greater confidence and control over the calls they answer.

For example, a call that is illegally “spoofed” – or shows a faked number – will fail the SHAKEN/STIR Caller ID verification and will not be marked as verified. By contrast, verification will confirm that a call is really coming from the identified number or entity. More calls will be verified over time as more device providers participate, and as more network providers implement the standards.

The FCC has recommended SHAKEN/STIR standards to digitally validate phone calls. The acronym stands for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR).

For more information on all the ways AT&T is protecting customers, visit https://about.att.com/story/2019/att_call_protect.html and <https://att.com/CyberAware>.

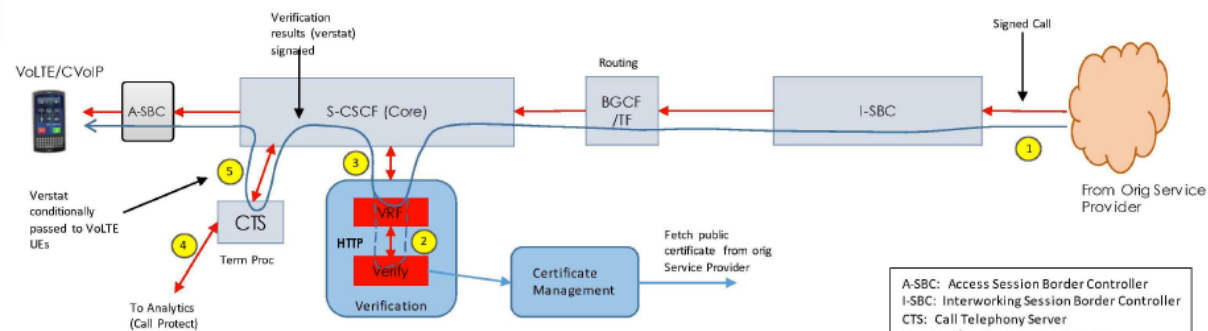
See also RQ0001970 (<https://sti-ga.atis.org/resources/>).

The terminating network conveys the verification result to the called user by including a "verstat" parameter in the From and/or P-Asserted-Identity header fields of the INVITE request sent to the called endpoint device, as defined in [TS 24.229].

- Call Validation Treatment (CVT) – This is a logical function that could be an application server function or a third party application for applying anti-spoofing mitigation techniques once the signature is positively or negatively verified. The CVT can also provide information in its response that indicates how the results of the verification should be displayed to the called user.

As another example, intra-network calls may be treated differently from inter-network calls. The attestation level of a call may be included within a verstat (verification indicator) tag, or other header. See e.g., ATT-RQ-466, 467.

Inter-Network SHAKEN Flows (ATT terminated)



1. Signed call is received from an originating carrier that supports SHAKEN. Terminating S-CSCF detects the received Identity header and sends the call to the VRF.
2. The VRF formulates the HTTP verification request and sends the request to the Verification Server.
3. The verification results are returned and signaled in the "verstat" parameter (contained in PAI/From headers).
4. Verstat is used by analytics (e.g. Call Protect) as an input to reputation scoring.
5. Verstat is conditionally passed to terminating VoLTE UE and UE uses this information to influence the calling number/name display information. For CVoIP, term CTS modifies the Calling Number to include SHAKEN verification results.

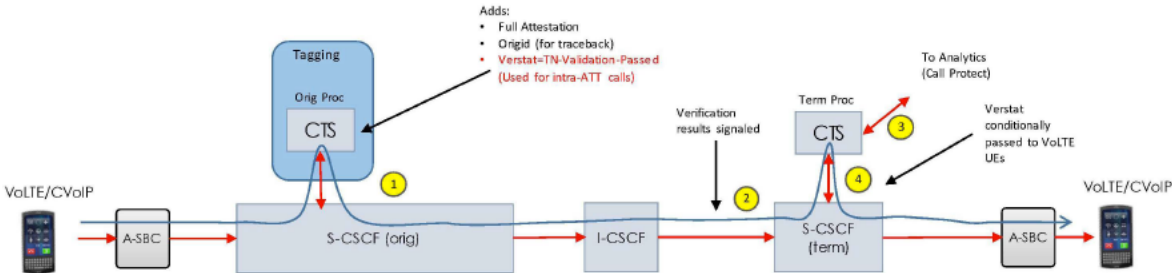
AT&T Proprietary and Confidential

This document and information contained therein is not for use or disclosure outside of AT&T

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY



ATT-RQ_0000466

	Intra-AT&T SHAKEN Flows  The diagram illustrates the Intra-AT&T SHAKEN Flows. It shows a call path starting from a VoLTE/CVoIP device, passing through an A-SBC, then an S-CSCF (orig), then an I-CSCF, then an S-CSCF (term), then another A-SBC, and finally to a VoLTE/CVoIP device. Key components include the Tagging process (Orig Proc CTS) and the Term Proc CTS. The flow is numbered 1 through 4, corresponding to the steps listed below. A legend box defines the acronyms: A-SBC: Access Session Border Controller, CTS: Call Telephony Server, I-CSCF: Interrogating Call Session Control Function, S-CSCF: Serving Call Session Control Function. A list of adds includes Full Attestation, OrigID (for traceback), and Verstat=TN-Validation-Passed (Used for intra-ATT calls). A note indicates that intra-ATT calls are not signed. Verification results are signaled, and Verstat is conditionally passed to VoLTE UEs. A final note states that Verstat is used by analytics (e.g., Call Protect) as an input to reputation scoring. - After originating processing is completed, CVoIP/VoLTE calls will be "tagged". - Tagging adds verstat parameter to emulate a call that was verified successfully. This is used for intra-network (ATT to ATT) calls. - Intra-ATT calls are not "signed". - The emulated verification result (verstat) is passed to CTS. - Verstat is used by analytics (e.g. Call Protect) as an input to reputation scoring. - Verstat is conditionally passed to terminating VoLTE UE and UE uses this information to influence the calling number/name display information. For CVoIP, term CTS modifies the Calling Number to include SHAKEN verification results. AT&T Proprietary and Confidential This document and information contained therein is not for use or disclosure outside of AT&T ATT-RQ_0000467
1[e] a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.	The Accused Instrumentalities comprise a memory coupled to the one or more processors and configured to provide the one or more processors with instructions. For example, the Accused Instrumentalities include one or more memories, including for example persistent memories (e.g., hard drives) and transient memories (e.g., random access memory), coupled to the one or more processors of the Accused Instrumentalities including via databases, which provide the one or more processors with instructions including instructions to perform the

	limitations of the claim. For further example, coupling also includes network infrastructure that couples memory and processor components across networks. <i>See, e.g.</i>, ATT-RQ_0000001 at 3 (showing volume of blocked calls necessitating the use of a memory coupled to one or more processors and configured to provide the one or more processors with instructions to make the determination to convey an assurance or failure to confirm): Hiya-AT&T Call Protect 2023 Summary  <table border="1"> <thead> <tr> <th>Category</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Calls Processed</td> <td>142 Billion</td> </tr> <tr> <td>Calls Flagged</td> <td>14 Billion</td> </tr> <tr> <td>Calls Blocked</td> <td>5.4 Billion</td> </tr> <tr> <td>Daily Calls Flagged</td> <td>38.4 Million</td> </tr> <tr> <td>Daily Calls Blocked</td> <td>14.8 Million</td> </tr> <tr> <td>Daily Calls Enriched</td> <td>389 Million</td> </tr> </tbody> </table> 3 DATA PROPRIETARY AND CONFIDENTIAL RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY hiya ATT-RQ_0000003 An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.	Category	Value	Calls Processed	142 Billion	Calls Flagged	14 Billion	Calls Blocked	5.4 Billion	Daily Calls Flagged	38.4 Million	Daily Calls Blocked	14.8 Million	Daily Calls Enriched	389 Million
Category	Value														
Calls Processed	142 Billion														
Calls Flagged	14 Billion														
Calls Blocked	5.4 Billion														
Daily Calls Flagged	38.4 Million														
Daily Calls Blocked	14.8 Million														
Daily Calls Enriched	389 Million														
Claim 2. The system recited in claim 1 wherein the information associated with the calling device is stored at an entity external to the calling device.	Within the Accused Instrumentalities the information associated with the calling device is stored at an entity external to the calling device. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).														

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. Feedback See also RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). For example, within the Accused Instrumentalities, the information associated with the calling device is stored external to the calling party, including at the Accused Instrumentalities and/or at other entities external to the calling device such as a Bluetooth-configured entity, a third-party entity, or an entity associated with the Accused Instrumentalities and/or under the direction and/or control of the Defendants.
--	--

	See, e.g., RQ-ATT0000070-RQ-ATT0000086 (https://about.att.com/privacy/privacy-notice.html). The information we collect × To better run our business, we collect information about you, your equipment and how you use our products and services. This can include: • Account information. You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including Customer Proprietary Network Information. • Equipment information. We collect information about equipment on our network like the type of device you use, device ID, and phone number. • Network performance. We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working. • Location information. Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites. • Web browsing and app information. We automatically collect a variety of information which may include time spent on websites or apps, website and IP addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information. • Biometric information. Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our Biometric Information Privacy Notice. • Third-party information. We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T.
--	---

	How we use your information x We rely on the information we collect to support our business functions, power our services and improve your experience, such as when we: • Combine it with the information from testing and running our network to determine which products and services better meet the needs of our customers. • Provide our products and services. • Contact you. • Improve your experience and safety. This includes verifying your identity, detecting and preventing fraud, protecting your financial accounts, authorizing transactions and assisting your interactions with customer care. • Improve and protect our network. • Use it to help understand which additional products and services may interest you and others. (We don’t access or use the content of your texts, emails or calls for this or any other marketing and advertising.) • Design and deliver advertising, marketing and promotional campaigns to you and others – and measuring their effectiveness (See your choices). • Use it for billing, collection, and protection of our property and legal rights. • Prevent and investigate security issues, illegal activities, and violations of our terms and conditions. • Conduct research and create aggregated reports – reports that offer insights about groups of customers, but not individuals (we do not attempt to re-identify individuals in aggregated reports). <i>See also</i> RQ-ATT0000139-RQ-ATT0000150 https://www.att.com/legal/terms.activeArmorMobileSecurity.html):
--	---

	In order to perform the functions of the Service including but not limited to its Call Features, AT&T may use and/or disclose or allow the disclosure to our third-party vendor(s) of Your personal information, including without limitation mobile number, contacts/address book in order to populate detail in the call detail screen, the presence or absence of calling party phone numbers in your Device address book, and App usage information, such as which numbers you report and/or manually block within the App, as factors to determine which callers are suspected fraud and spam. The contact names and phone numbers in your Device address book are not shared for any purpose other than improving your experience with the App by helping you to recognize known callers. 3.2 Consent for Information Disclosure in Connection with Data Features The Service includes the following data security and related features: Device Security Alerts, Data Breach Alerts, Public Wi-Fi Protection (VPN & Wi-Fi Alerts), Identity Monitoring, Reverse Number Lookup, Safe Browsing, and Device Theft Alerts (collectively “Data Features”) In order to perform the functions and to improve the effectiveness of the Service including but not limited to its Data Features for all users, AT&T, its pertinent suppliers and their subsidiaries, agents and subcontractors may collect, maintain, process, use, and disclose diagnostic, technical, usage and related information including, but not limited to, information about: • the type of Device You are using and the operating system You are running; • Your applicable wireless network provider/carrier; • the applications and files present on Your Device and SD memory card; • the results of any scans performed by the App; and • actions You take as a result of any virus or malware notifications. We also may collect information about how the App and any associated Service applications behave on Your Device and the network services with which applications installed on Your Device communicate in order to determine if any applications are behaving maliciously (for example, is an application accessing Your address contacts, sending premium-rate text messages that charge money to Your wireless bill, or communicating with a server known to host phishing websites). <i>See, e.g.,</i> RQ-ATT0000051-RQ-ATT0000053 (https://about.att.com/story/2019/att_tmo_call-authentication.html).
--	--

AT&T* and T-Mobile today began rollout of cross-network call authentication based on SHAKEN/STIR standards – another big step toward protecting consumers from unwanted robocalls.

SHAKEN/STIR technology lets consumers know that an incoming call is really coming from the number listed on the caller ID display – not a spoofed robocall or scammer. While authentication won’t solve the problem of unwanted robocalls by itself, it is a key step toward giving customers greater confidence and control over the calls they answer.

For example, a call that is illegally “spoofed” – or shows a faked number – will fail the SHAKEN/STIR Caller ID verification and will not be marked as verified. By contrast, verification will confirm that a call is really coming from the identified number or entity. More calls will be verified over time as more device providers participate, and as more network providers implement the standards.

The FCC has recommended SHAKEN/STIR standards to digitally validate phone calls. The acronym stands for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR).

For more information on all the ways AT&T is protecting customers, visit https://about.att.com/story/2019/att_call_protect.html and <https://att.com/CyberAware>.

	As one example, at least part of the information associated with the SIP Identity header may be stored at an entity external to the calling device. As another example, at least part of the encoding information may be stored at an entity external to the calling device. An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 3. The system recited in claim 1 wherein the information associated with the calling device comprises a cryptographic key associated with the calling device.	Within the Accused Instrumentalities the information associated with the calling device comprises a cryptographic key associated with the calling device. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. Feedback CHAT See also RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, within the Accused Instrumentalities, the information associated with the calling device comprises a cryptographic key associated with the calling device or otherwise belonging to the calling device, including a cryptographic key for calling device communications that include information associated with the calling device that is encrypted and/or requires authentication. As another example, the SIP Identity header comprises a cryptographic key associated with the calling device. As yet another example, the Personal Assertion Token (PASSport), which is a value generated based at least in part on information associated with the calling device, contains a cryptographic key associated with the calling device.
--	--

	An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 4. The system recited in claim 1 wherein the value is generated based at least in part on one of symmetric key cryptography and asymmetric key cryptography.	Within the Accused Instrumentalities the value is generated based at least in part on one of symmetric key cryptography and asymmetric key cryptography. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/). How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req’s compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req’s apply. Details at att.com/activearmorapp. Feedback

	<i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the value is generated based at least in part on one of symmetric key cryptography and asymmetric key cryptography. As one example, the Personal Assertion Token (PASSporT), which is a value, is generated based at least in part on one of symmetric key cryptography and asymmetric key cryptography. <i>See, e.g.,</i> RQ0002017-RQ0002041 (https://datatracker.ietf.org/doc/html/rfc8225). An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 5. The system recited in claim 1 wherein the score for the calling device is generated in response to the call being initiated by the calling device.	Within the Accused Instrumentalities the score for the calling device is generated in response to the call being initiated by the calling device. The score generated in response to the call being initiated may be generated by Defendants, a third party (e.g., Hiya), or some combination thereof. The score can be generated by one or more machine learning algorithms in response to the call being initiated by the calling device. <i>See e.g.,</i> https://work.hiya.com/adaptive-ai-ebook

Adaptive AI: A Proactive Strategy for Stopping Scam and Fraud Calls

Adaptive AI is an innovative new feature of Hiya Protect, a proprietary call protection service used by carriers, distribution partners and the Hiya mobile app.

Unlike other capabilities on the market today, Adaptive AI uses machine learning to proactively hunt and shut down scam campaigns. With the ability to stay ahead of scammers, Adaptive AI works in real-time, without the need for human intervention or any updating of existing AI models.

For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (<https://www.att.com/security/>).

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. <i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As another example, Enterprise Caller Scoring is a score generated for the calling device that indicates the validity of a phone number. <i>See, e.g.,</i> https://www.hiya.com/products/enterprise-caller-scoring:
--	---

How it Works

Enterprise Caller Scoring is a new layer of Hiya's Adaptive AI that stops number rotation — the practice of switching phone numbers to avoid spam detection — from being effective on mobile networks.

Like a credit agency for enterprise callers, Enterprise Caller Scoring assesses incoming calls based on the calling enterprise's history across all the numbers they own. It can identify the calling enterprise's reputation for more than 150 million enterprise phone numbers in the US — even phone numbers that haven't yet built a calling history. An enterprise's reputation continuously evolves based on behavior and is automatically recognized across all their numbers.

See also <https://blog.hiya.com/how-hiyas-proprietary-adaptive-ai-stops-phone-spam>.

As another example, within the Accused Instrumentalities, the received information pertaining to the call includes a score generated for the calling device, the score indicating a validity of a phone

number and being generated in response to the call being initiated by the calling device. For example, the score generated for the calling device comprises, and/or has as an input or signal among other inputs and/or signals, an indication of the attestation level associated with the calling device and indicates validity of a phone number, but the score is not limited to the A or B or C attestation level.

For example, the score for the calling device comprises and/or has as an input or signal, among other inputs and/or signals, an indication of the attestation level associated with the calling device and is generated in response to the call being initiated by the calling device, but the score is not limited to the A or B or C attestation level. *See, e.g.*, RQ0001970 (<https://sti-ga.atis.org/resources/>).

5.2.3 Attestation Indicator (“attest”)

The “attest” claim allows the originating service provider that is populating an Identity header to clearly indicate the information it can vouch for regarding the origination of the call.

~~This indicator allows for both identifying the service provider that is vouching for the call as well as clearly indicating what information the service provider is attesting to.~~

In the SHAKEN framework we define the following three levels of attestation:

A. Full Attestation: The signing provider shall satisfy all of the following conditions:

- Is responsible for the origination of the call onto the IP_-based service provider voice network.
- Has a direct authenticated relationship with the customer and can identify the customer.
- Has established a verified association with the telephone number used for the call.

NOTE 1: The signing provider is asserting that their customer can “legitimately” use the number that appears as the calling party (i.e., the Caller ID). The legitimacy of the telephone number(s) the originator of the call can use is subject to signer-specific policy, but could use mechanisms such as the following:

- The number was assigned to this customer by the signing service provider.
- This number is one of a range of numbers assigned to an enterprise or wholesale customer.
- The signing service provider has ascertained that the customer is authorized to use a number (e.g., by business agreement or evidence the customer has access to use the number). This includes numbers assigned by another service provider.
- The number is not permanently assigned to an individual customer but the signing provider can track the use of the number by a customer for certain calls or during a certain timeframe.

NOTE 2: Ultimately it is up to service provider policy to decide what constitutes “legitimate right to assert a telephone number” but the service provider’s reputation may be directly dependent on how rigorous they have been in making this assertion.

	B. Partial Attestation: The signing provider shall satisfy all of the following conditions: • Is responsible for the origination of the call onto ~~its-the~~ IP-based <u>service provider</u> voice network. • Has a direct authenticated relationship with the customer and can identify the customer. • Has NOT established a verified association with the telephone number being used for the call. 9 ATIS-1000074-E -- SIP Forum TWG-10-E ~~NOTE: By populating this value, the service provider attests that it can trace the source of the call to a customer for policy enforcement purposes. When partial attestation is used, each customer will have a unique origination identifier created and managed by the service provider, but the intention is that it will not be possible to reverse engineer the identity of the customer purely from the identifier or signature. As described in section 5.2.4, the unique origination identifier allows data analytics to establish a reputation profile and assess the reliability of information asserted by the customer assigned this unique identifier. The identifier also provides a reliable mechanism to determine the customer for forensic analysis or legal action where appropriate.~~ An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 6. The system recited in claim 1, wherein the score for the calling device is generated based at least in part on information associated with a user that is associated with the calling device.	Within the Accused Instrumentalities the score for the calling device is generated based at least in part on information associated with a user that is associated with the calling device. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” See, e.g., RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. <i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As another example, Enterprise Caller Scoring is a score generated for the calling device that indicates the validity of a phone number and is based upon reputation, which is information associated with a user that is associated with the calling device. For instance, whenever a call is made, Enterprise Caller Scoring uses the calling number to look up the reputation of the calling business — even if that number has been recently rotated into use. Enterprise Caller Scoring continuously evolves caller reputation based on behavior, so businesses can maintain and grow their reputations over time
--	--

through disciplined calling practices — without the need to rely on spam evasion services that utilize number rotation. *See, e.g.,* <https://www.hiya.com/products/enterprise-caller-scoring>:

How it Works

Enterprise Caller Scoring is a new layer of Hiya's Adaptive AI that stops number rotation — the practice of switching phone numbers to avoid spam detection — from being effective on mobile networks.

Like a credit agency for enterprise callers, Enterprise Caller Scoring assesses incoming calls based on the calling enterprise's history across all the numbers they own. It can identify the calling enterprise's reputation for more than 150 million enterprise phone numbers in the US — even phone numbers that haven't yet built a calling history. An enterprise's reputation continuously evolves based on behavior and is automatically recognized across all their numbers.

See also <https://blog.hiya.com/how-hiyas-proprietary-adaptive-ai-stops-phone-spam>.

	As another example, the score for the calling device is generated based at least in part on information associated with a user that is associated with the calling device. As an example, the score is generated based on prior actions by the user that is associated with the device. As another example, the score is generated based upon reports of the user associated with the device making spoof calls. As another example, the score is generated on the information, such as the telephone number, or other account information, associated with a user of the calling device. As another example, the score for the calling device is generated based at least in part on the following information that is associated with a user that is associated with the calling device: a mobile identification number (“MIN”) or any derivation of a MIN or any related number; mobile subscription identification number (“MSIN”); an international mobile subscriber identity (“IMSI”) or encrypted version thereof (“TMSI”); Subscriber Module (SIM) Card serial number; serial number, Host Device ID, or any other unique identifier for a device (including but not limited to Android ID, UDID, IDFA, AAID). As another example, the score of the calling device is generated based at least in part on the following information associated with a user that is associated with the calling device: <i>See, e.g.</i>, RQ-ATT0000070-RQ-ATT0000086 (https://about.att.com/privacy/privacy-notice.html).
--	---

	The information we collect x To better run our business, we collect information about you, your equipment and how you use our products and services. This can include: • Account information. You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including Customer Proprietary Network Information. • Equipment information. We collect information about equipment on our network like the type of device you use, device ID, and phone number. • Network performance. We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working. • Location information. Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites. • Web browsing and app information. We automatically collect a variety of information which may include time spent on websites or apps, website and IP addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information. • Biometric information. Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our Biometric Information Privacy Notice. • Third-party information. We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T.
--	--

	How we use your information x We rely on the information we collect to support our business functions, power our services and improve your experience, such as when we: • Combine it with the information from testing and running our network to determine which products and services better meet the needs of our customers. • Provide our products and services. • Contact you. • Improve your experience and safety. This includes verifying your identity, detecting and preventing fraud, protecting your financial accounts, authorizing transactions and assisting your interactions with customer care. • Improve and protect our network. • Use it to help understand which additional products and services may interest you and others. (We don’t access or use the content of your texts, emails or calls for this or any other marketing and advertising.) • Design and deliver advertising, marketing and promotional campaigns to you and others – and measuring their effectiveness (See your choices). • Use it for billing, collection, and protection of our property and legal rights. • Prevent and investigate security issues, illegal activities, and violations of our terms and conditions. • Conduct research and create aggregated reports – reports that offer insights about groups of customers, but not individuals (we do not attempt to re-identify individuals in aggregated reports). <i>See also</i> RQ-ATT0000139-RQ-ATT0000150 https://www.att.com/legal/terms.activeArmorMobileSecurity.html):
--	---

	In order to perform the functions of the Service including but not limited to its Call Features, AT&T may use and/or disclose or allow the disclosure to our third-party vendor(s) of Your personal information, including without limitation mobile number, contacts/address book in order to populate detail in the call detail screen, the presence or absence of calling party phone numbers in your Device address book, and App usage information, such as which numbers you report and/or manually block within the App, as factors to determine which callers are suspected fraud and spam. The contact names and phone numbers in your Device address book are not shared for any purpose other than improving your experience with the App by helping you to recognize known callers. 3.2 Consent for Information Disclosure in Connection with Data Features The Service includes the following data security and related features: Device Security Alerts, Data Breach Alerts, Public Wi-Fi Protection (VPN & Wi-Fi Alerts), Identity Monitoring, Reverse Number Lookup, Safe Browsing, and Device Theft Alerts (collectively “Data Features”) In order to perform the functions and to improve the effectiveness of the Service including but not limited to its Data Features for all users, AT&T, its pertinent suppliers and their subsidiaries, agents and subcontractors may collect, maintain, process, use, and disclose diagnostic, technical, usage and related information including, but not limited to, information about: • the type of Device You are using and the operating system You are running; • Your applicable wireless network provider/carrier; • the applications and files present on Your Device and SD memory card; • the results of any scans performed by the App; and • actions You take as a result of any virus or malware notifications. We also may collect information about how the App and any associated Service applications behave on Your Device and the network services with which applications installed on Your Device communicate in order to determine if any applications are behaving maliciously (for example, is an application accessing Your address contacts, sending premium-rate text messages that charge money to Your wireless bill, or communicating with a server known to host phishing websites). The score generated for the calling device comprises an indication of the attestation level associated with the calling device. <i>See, e.g.</i>, RQ0001970 (https://sti-ga.atis.org/resources/).
--	--

5.2.3 Attestation Indicator (“attest”)

The “attest” claim allows the originating service provider that is populating an Identity header to clearly indicate the information it can vouch for regarding the origination of the call.

~~This indicator allows for both identifying the service provider that is vouching for the call as well as clearly indicating what information the service provider is attesting to.~~

In the SHAKEN framework we define the following three levels of attestation:

A. Full Attestation: The signing provider shall satisfy all of the following conditions:

- Is responsible for the origination of the call onto the IP-based service provider voice network.
- Has a direct authenticated relationship with the customer and can identify the customer.
- Has established a verified association with the telephone number used for the call.

NOTE 1: The signing provider is asserting that their customer can “legitimately” use the number that appears as the calling party (i.e., the Caller ID). The legitimacy of the telephone number(s) the originator of the call can use is subject to signer-specific policy, but could use mechanisms such as the following:

- The number was assigned to this customer by the signing service provider.
- This number is one of a range of numbers assigned to an enterprise or wholesale customer.
- The signing service provider has ascertained that the customer is authorized to use a number (e.g., by business agreement or evidence the customer has access to use the number). This includes numbers assigned by another service provider.
- The number is not permanently assigned to an individual customer but the signing provider can track the use of the number by a customer for certain calls or during a certain timeframe.

NOTE 2: Ultimately it is up to service provider policy to decide what constitutes “legitimate right to assert a telephone number” but the service provider’s reputation may be directly dependent on how rigorous they have been in making this assertion.

	B. Partial Attestation: The signing provider shall satisfy all of the following conditions: • Is responsible for the origination of the call onto ~~its~~-the IP-based <u>service provider</u> voice network. • Has a direct authenticated relationship with the customer and can identify the customer. • Has NOT established a verified association with the telephone number being used for the call. 9 ATIS-1000074-E -- SIP Forum TWG-10-E <u>NOTE: By populating this value, the service provider attests that it can trace the source of the call to a customer for policy enforcement purposes.</u>~~When partial attestation is used, each customer will have a unique origination identifier created and managed by the service provider, but the intention is that it will not be possible to reverse engineer the identity of the customer purely from the identifier or signature. As described in section 5.2.4, the unique origination identifier allows data analytics to establish a reputation profile and assess the reliability of information asserted by the customer assigned this unique identifier. The identifier also provides a reliable mechanism to determine the customer for forensic analysis or legal action where appropriate.~~ An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 7. The system recited in claim 1 wherein the information pertaining to the call further includes at least one of a timestamp associated with the call and a called phone number.	Within the Accused Instrumentalities the information pertaining to the call further includes at least one of a timestamp associated with the call and a called phone number. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” See, e.g., RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/). The information pertaining to the call used by Verizon to combat Robocalls, SPAM and fraudulent phone calls includes at least one of a timestamp associated with the call and a called phone number.

How do AT&T and the other major carriers differ in terms of security? ^

AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.

To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost.

ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited

Req’s compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req’s apply. Details at att.com/activearmorapp.

Feedback



See also RQ-ATT0000012-RQ-ATT0000023 (<https://sustainability.att.com/priority-topics/network-data-security>).

As another example, in the Accused Instrumentalities, the SIP INVITE includes timing parameters that constitute a timestamp associated with the call, including but not limited to a timestamp, the “iat” attribute, a counter, a nonce, Invite request retransmit interval, Invite transaction timeout timer, and/or any other SIP invitation timing parameter, *See, e.g., SIP Identity Header*, CarrierX, RQ0001945-RQ0001948 (<https://www.carrierx.com/documentation/how-it-works/stir-shaken#sip-identity-header>). For another example, in the Accused Instrumentalities, the SIP INVITE includes

	a called phone number, including the “dest” attribute and/or any object containing the tn array or that otherwise lists the destination numbers or called URIs. <i>See, e.g.</i>, RQ0001945-RQ0001948 (https://www.carrierx.com/documentation/how-it-works/stir-shaken#sip-identity-header). An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 8. The system recited in claim 1 wherein the security determination is performed by one of a device associated with a called phone number and an entity different from the device associated with a called phone number.	Within the Accused Instrumentalities the security determination is performed by one of a device associated with a called phone number and an entity different from the device associated with a called phone number. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. <i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the security determination is performed by the Accused Instrumentalities, which is an entity different from the callee’s device associated with the called phone number. As another example, the Accused Instrumentalities comprise one or more devices that can be associated with a called number so that the security determination is performed by a device associated with a called number. As another example, the security determination is performed at Defendants’ direction and/or control by a third party entity (e.g. Hiya) that is different from the device associated with a called phone number.
--	---

	An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 9. The system recited in claim 1 wherein the security determination comprises determining a validity of the call based at least in part on a cryptographic key on the calling device.	Within the Accused Instrumentalities the security determination comprises determining a validity of the call based at least in part on a cryptographic key on the calling device. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/). How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req’s compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req’s apply. Details at att.com/activearmorapp. <i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security).

	As one example, the cryptographic key is on the device so that the device can transmit a SIP INVITE with cryptographic information (e.g., branch identification or “branch id”). <i>See Generating Call-ID, From and To tags, Branch-ID and Cseq</i>, Oracle, RQ0001956 (https://docs.oracle.com/cd/E36784_01/html/E36863/makehtml-id-10.html). As another example, the cryptographic key is a random or unique number from the device that allows a security determination. As another example, the security determination comprises determining a validity of the call based on the branch id as it is a unique number that serves as a cryptographic key by allowing a determination on the validity of the request. As yet another example, the security determination comprises determining a validity of the call based at least in part on a cryptographic key on the calling device such as the seed value, which is used to generate pseudo-random values by the device. <i>See Random seed</i>, Wikipedia, https://en.wikipedia.org/wiki/Random_seed. <i>See also Example SIP INVITE</i>, Twilio Docs, RQ0002066-RQ0002080 (https://www.twilio.com/docs/glossary/sip-invites#example-sip-invite); <i>SIP forking</i>, Tutorialspoint, RQ0002061-RQ0002065 (https://www.tutorialspoint.com/session_initiation_protocol/session_initiation_protocol_forking.htm); Josh Whitaker, Beginner’s guide to SIP headers [Complete list], Telnyx (Sept. 29, 2023), RQ0001666-RQ0001671 (https://telnyx.com/resources/the-beginners-guide-to-sip-headers). As another example, the device may send a cryptographic key. An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 10. The system recited in claim 1 wherein the information pertaining to the call further includes a timestamp, and wherein the one or more processors are configured to prevent a replay attack using the timestamp.	Within the Accused Instrumentalities the information pertaining to the call further includes a timestamp, and the one or more processors are configured to prevent a replay attack using the timestamp. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. Feedback See also RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, in the Accused Instrumentalities, the information pertaining to the call includes the SIP INVITE includes timing parameters that constitute a timestamp, including but not limited to a timestamp, counter, nonce, Invite request retransmit interval, Invite transaction timeout timer, or any other SIP invitation timing parameters, and the one or more processors of the Accused Instrumentalities are configured to prevent a replay attack using the timestamp. See, e.g., RFC 8224 (directing that a PASSporT for a SIP request “MUST NOT [be] generated . . . if the Date header is
--	--

	outside of its local policy for freshness (sixty seconds is RECOMMENDED”). An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 11. The system recited in claim 1 wherein the security determination is based at least in part on a score indicating a validity of the call, and wherein the score is generated based at least in part on device information.	Within the Accused Instrumentalities wherein the security determination is based at least in part on a score indicating a validity of the call, and wherein the score is generated based at least in part on device information. As one example, the received information pertaining to the call includes a score generated for the calling device, the score indicating a validity of a phone number. The score generated for the calling device may be scored from Defendants, a third party (e.g. Hiya), or some combination thereof. The score can be generated by one or more machine learning algorithms. <i>See e.g.</i>, https://work.hiya.com/adaptive-ai-ebook

Adaptive AI: A Proactive Strategy for Stopping Scam and Fraud Calls

Adaptive AI is an innovative new feature of Hiya Protect, a proprietary call protection service used by carriers, distribution partners and the Hiya mobile app.

Unlike other capabilities on the market today, Adaptive AI uses machine learning to proactively hunt and shut down scam campaigns. With the ability to stay ahead of scammers, Adaptive AI works in real-time, without the need for human intervention or any updating of existing AI models.

Furthermore, the score is generated based at least in part on information associated with the calling device can include a device fingerprint, device information (e.g., make, model, serial number, operating system version, application information, or other identifying information of a device), customer account information, location information, or other information associated with the device.

For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (<https://www.att.com/security/>).

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. <i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the security determination is based at least in part on a score indicating a validity of the call, and wherein the score is generated based at least in part on device information by Defendants, a third party (e.g. Hiya) or some combination thereof. As another example, Enterprise Caller Scoring is a score generated for the calling device that indicates the validity of a phone number. <i>See, e.g.,</i> https://www.hiya.com/products/enterprise-caller-scoring:
--	--

How it Works

Enterprise Caller Scoring is a new layer of Hiya's Adaptive AI that stops number rotation — the practice of switching phone numbers to avoid spam detection — from being effective on mobile networks.

Like a credit agency for enterprise callers, Enterprise Caller Scoring assesses incoming calls based on the calling enterprise's history across all the numbers they own. It can identify the calling enterprise's reputation for more than 150 million enterprise phone numbers in the US — even phone numbers that haven't yet built a calling history. An enterprise's reputation continuously evolves based on behavior and is automatically recognized across all their numbers.

See also <https://blog.hiya.com/how-hiyas-proprietary-adaptive-ai-stops-phone-spam>.

As one example, the score generated based at least in part on device information is information provided by Defendants, a third party (e.g., Hiya), or some combination thereof. *See* ATT-RQ_0000042, -43, -44 (evidencing fingerprint information such device specific data, device settings, installed applications (e.g., ActiveArmor), system or application software versions (“Device OS”, “ActiveArmor Version Information”), contact list data (TN from Device Address Book), or other data specific to the calling device is stored and shared with AT&T’s “Vendor/Partner Hiya”):

Active Armor Data Elements

As part of the Active Armor Robocall mitigation program, data elements related to calling are shared with our Vendor/Partner Hiya. Note that Hiya’s usage and management of these data elements is under written agreement with AT&T.

AT&T GFMO (Global Fraud Management Office) and AT&T CDO (Chief Data Office) each provide a set of per-Number data elements. AT&T CTS/PRS uses an API to provide per-Call data elements. There are additional data elements that are under investigation to determine if they will have value in Robocall Mitigation.

The following is a listing of each data element, by data source. See attached spreadsheet for more details.

AT&T CTS/PRS**Call Direction Response API (Per Call Basis)**

callEventNotification
notificationType
eventDescription
correlationId
callingParticipant
callingParticipantName
callingParticipantAlternate
calledParticipant
callingParticipantPrivacy
callSessionIdentifier
addressDirection:
originatorTasId:
callingParticipantAccessNetworkInfo
callbackData
link

action
actionToPerform
displayName
routingAddress
decisionId
displayAddress
callInfo

These are additional Parameters Call Direction Response API (CR 245)

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

CTN (including AT&T/FN/Cricket customers)

Service tier (like Basic vs. Advanced)

Service Tags:

- FirstNet
- CRU
- COU
- Customers who have rate-plan-included Advanced service.
- Cricket
- Prepaid
- Wireless Home Phone

ActiveArmor Application Data

TN from Device Address Book - Hashed (shared only with explicit subscriber consent)

Device OS

ActiveArmor Version Information

As another example, the security determination is based at least in part on a score indicating a validity of the call, and the score is generated based at least in part on device information. As another example, the security determination is based at least in part on the attestation level associated with

the calling device, and the attestation level is generated based at least in part on device information and/or information associated with the calling device. *See, e.g.,* RQ0001970 (<https://stiga.atis.org/resources/>). While the scoring from Defendants, a third-party, or a combination thereof indicates the validity of a phone number that may comprise an indication of an attestation level, the score is not limited to only A or B or C.

5.2.3 Attestation Indicator (“attest”)

The “attest” claim allows the originating service provider that is populating an Identity header to clearly indicate the information it can vouch for regarding the origination of the call.

~~This indicator allows for both identifying the service provider that is vouching for the call as well as clearly indicating what information the service provider is attesting to.~~

In the SHAKEN framework we define the following three levels of attestation:

A. Full Attestation: The signing provider shall satisfy all of the following conditions:

- Is responsible for the origination of the call onto the IP-based service provider voice network.
- Has a direct authenticated relationship with the customer and can identify the customer.
- Has established a verified association with the telephone number used for the call.

NOTE 1: The signing provider is asserting that their customer can “legitimately” use the number that appears as the calling party (i.e., the Caller ID). The legitimacy of the telephone number(s) the originator of the call can use is subject to signer-specific policy, but could use mechanisms such as the following:

- The number was assigned to this customer by the signing service provider.
- This number is one of a range of numbers assigned to an enterprise or wholesale customer.
- The signing service provider has ascertained that the customer is authorized to use a number (e.g., by business agreement or evidence the customer has access to use the number). This includes numbers assigned by another service provider.
- The number is not permanently assigned to an individual customer but the signing provider can track the use of the number by a customer for certain calls or during a certain timeframe.

NOTE 2: Ultimately it is up to service provider policy to decide what constitutes “legitimate right to assert a telephone number” but the service provider’s reputation may be directly dependent on how rigorous they have been in making this assertion.

	B. Partial Attestation: The signing provider shall satisfy all of the following conditions: • Is responsible for the origination of the call onto ~~its~~ <u>the</u> IP-based <u>service provider</u> voice network. • Has a direct authenticated relationship with the customer and can identify the customer. • Has NOT established a verified association with the telephone number being used for the call. 9 ATIS-1000074-E -- SIP Forum TWG-10-E <u>NOTE: By populating this value, the service provider attests that it can trace the source of the call to a customer for policy enforcement purposes</u>~~When partial attestation is used, each customer will have a unique origination identifier created and managed by the service provider, but the intention is that it will not be possible to reverse engineer the identity of the customer purely from the identifier or signature. As described in section 5.2.4, the unique origination identifier allows data analytics to establish a reputation profile and assess the reliability of information asserted by the customer assigned this unique identifier. The identifier also provides a reliable mechanism to determine the customer for forensic analysis or legal action where appropriate.~~ An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 12. The system recited in claim 1 wherein the device information used to generate the score comprises at least one of a unique software identifier, a semi-unique software identifier, an embedded hardware identifier, a user-added hardware identifier, and a device fingerprint.	Within the Accused Instrumentalities the device information used to generate the score comprises at least one of a unique software identifier, a semi-unique software identifier, an embedded hardware identifier, a user-added hardware identifier, and a device fingerprint. For example, the device information used to generate the score in the Accused Instrumentalities includes a device fingerprint. <i>See</i> ATT-RQ_0000042, -43, -44 (evidencing fingerprint information such as device specific data, device settings, installed applications (e.g., ActiveArmor), system or application software versions (“Device OS”, “ActiveArmor Version Information”), contact list data (TN from Device Address Book), or other data specific to the calling device is stored and shared

with AT&T’s “Vendor/Partner Hiya.”):

Active Armor Data Elements

As part of the Active Armor Robocall mitigation program, data elements related to calling are shared with our Vendor/Partner Hiya. Note that Hiya’s usage and management of these data elements is under written agreement with AT&T.

AT&T GFMO (Global Fraud Management Office) and AT&T CDO (Chief Data Office) each provide a set of per-Number data elements. AT&T CTS/PRS uses an API to provide per-Call data elements. There are additional data elements that are under investigation to determine if they will have value in Robocall Mitigation.

The following is a listing of each data element, by data source. See attached spreadsheet for more details.

AT&T CTS/PRS**Call Direction Response API (Per Call Basis)**

callEventNotification
 notificationType
 eventDescription
 correlationId
 callingParticipant
 callingParticipantName
 callingParticipantAlternate
 calledParticipant
 callingParticipantPrivacy
 callSessionIdentifier
 addressDirection:
 originatorTasId:
 callingParticipantAccessNetworkInfo
 callbackData
 link

 action
 actionToPerform
 displayName
 routingAddress
 decisionId
 displayAddress
 callInfo

These are additional Parameters Call Direction Response API (CR 245)

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

CTN (including AT&T/FN/Cricket customers)

Service tier (like Basic vs. Advanced)

Service Tags:

- FirstNet
- CRU
- COU
- Customers who have rate-plan-included Advanced service.
- Cricket
- Prepaid
- Wireless Home Phone

ActiveArmor Application Data

TN from Device Address Book - Hashed (shared only with explicit subscriber consent)

Device OS

ActiveArmor Version Information

For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” See, e.g., RQ-ATT0000035-RQ-ATT0000041 (<https://www.att.com/security/>).

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. <i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the device information used to generate the score comprises at least one of a unique software identifier, a semi-unique software identifier, an embedded hardware identifier, a user-added hardware identifier, and/or a device fingerprint. For example, SIM information can be hardware, such as a SIM card, or software, such as data. <i>See, e.g.,</i> SIM card, <i>Wikipedia</i>, RQ0002042-RQ0002060 (https://en.wikipedia.org/wiki/SIM_card). As another example, the device information used to generate the attestation level comprises a unique software identifier. As another example,
--	--

	the device information used to generate the attestation level comprises a semi-unique software identifier. As another example, the device information used to generate the attestation level comprises an embedded hardware identifier. As another example, the device information used to generate the attestation level comprises a user-added hardware identifier. As another example, the device information used to generate the attestation level comprises a device fingerprint. As another example, in the Accused Instrumentalities, the following device information and/or any combination thereof or in combination with the device information set forth below, which comprises one of a unique software identifier, a semi-unique software identifier, an embedded hardware identifier, a user-added hardware identifier, and/or a device fingerprint, is used to generate the score, including the attestation level and/or any other score within the Accused Instrumentalities: a mobile identification number (“MIN”) or any derivation of a MIN or any related number; mobile subscription identification number (“MSIN”); an international mobile subscriber identity (“IMSI”) or encrypted version thereof (“TMSI”); Subscriber Module (SIM) Card serial number; serial number, Host Device ID, or any other unique identifier for a device (including but not limited to Android ID, UDID, IDFA, AAID). As another example, in the Accused Instrumentalities, the following device information and/or any combination thereof or in combination with the device information set forth above, which comprises one of a unique software identifier, a semi-unique software identifier, an embedded hardware identifier, a user-added hardware identifier, and/or a device fingerprint, is used to generate the score, including the attestation level and/or any other score within the Accused Instrumentalities: <i>See, e.g.,</i> RQ-ATT0000070-RQ-ATT0000086 (https://about.att.com/privacy/privacy-notice.html).
--	---

	The information we collect × To better run our business, we collect information about you, your equipment and how you use our products and services. This can include: • Account information. You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including Customer Proprietary Network Information. • Equipment information. We collect information about equipment on our network like the type of device you use, device ID, and phone number. • Network performance. We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working. • Location information. Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites. • Web browsing and app information. We automatically collect a variety of information which may include time spent on websites or apps, website and IP addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information. • Biometric information. Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our Biometric Information Privacy Notice. • Third-party information. We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T.
--	--

	How we use your information × We rely on the information we collect to support our business functions, power our services and improve your experience, such as when we: • Combine it with the information from testing and running our network to determine which products and services better meet the needs of our customers. • Provide our products and services. • Contact you. • Improve your experience and safety. This includes verifying your identity, detecting and preventing fraud, protecting your financial accounts, authorizing transactions and assisting your interactions with customer care. • Improve and protect our network. • Use it to help understand which additional products and services may interest you and others. (We don’t access or use the content of your texts, emails or calls for this or any other marketing and advertising.) • Design and deliver advertising, marketing and promotional campaigns to you and others – and measuring their effectiveness (See your choices). • Use it for billing, collection, and protection of our property and legal rights. • Prevent and investigate security issues, illegal activities, and violations of our terms and conditions. • Conduct research and create aggregated reports – reports that offer insights about groups of customers, but not individuals (we do not attempt to re-identify individuals in aggregated reports). <i>See also</i> RQ-ATT0000139-RQ-ATT0000150 (https://www.att.com/legal/terms.activeArmorMobileSecurity.html):
--	---

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

	In order to perform the functions of the Service including but not limited to its Call Features, AT&T may use and/or disclose or allow the disclosure to our third-party vendor(s) of Your personal information, including without limitation mobile number, contacts/address book in order to populate detail in the call detail screen, the presence or absence of calling party phone numbers in your Device address book, and App usage information, such as which numbers you report and/or manually block within the App, as factors to determine which callers are suspected fraud and spam. The contact names and phone numbers in your Device address book are not shared for any purpose other than improving your experience with the App by helping you to recognize known callers. 3.2 Consent for Information Disclosure in Connection with Data Features The Service includes the following data security and related features: Device Security Alerts, Data Breach Alerts, Public Wi-Fi Protection (VPN & Wi-Fi Alerts), Identity Monitoring, Reverse Number Lookup, Safe Browsing, and Device Theft Alerts (collectively “Data Features”) In order to perform the functions and to improve the effectiveness of the Service including but not limited to its Data Features for all users, AT&T, its pertinent suppliers and their subsidiaries, agents and subcontractors may collect, maintain, process, use, and disclose diagnostic, technical, usage and related information including, but not limited to, information about: • the type of Device You are using and the operating system You are running; • Your applicable wireless network provider/carrier; • the applications and files present on Your Device and SD memory card; • the results of any scans performed by the App; and • actions You take as a result of any virus or malware notifications. We also may collect information about how the App and any associated Service applications behave on Your Device and the network services with which applications installed on Your Device communicate in order to determine if any applications are behaving maliciously (for example, is an application accessing Your address contacts, sending premium-rate text messages that charge money to Your wireless bill, or communicating with a server known to host phishing websites). An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 13. The system recited in claim 12 wherein the user-added hardware identifier is associated with geolocation information.	Within the Accused Instrumentalities the user-added hardware identifier is associated with geolocation information. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.”

See, e.g., RQ-ATT0000035-RQ-ATT0000041 (<https://www.att.com/security/>).

How do AT&T and the other major carriers differ in terms of security? ^

AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.

To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost.

ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited

Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp.

Feedback



See also RQ-ATT0000012-RQ-ATT0000023 (<https://sustainability.att.com/priority-topics/network-data-security>).

As one example, the user-added hardware identifier is associated with geolocation information, such as specific country information that can be used for verification purposes. As one example, the user-added hardware identifier has geolocation information, providing the location of the user. As another example, the user-added hardware identifier becomes associated with geolocation information. As

	yet another example, the user-added hardware identifier becomes associated with geolocation information because this information is stored on the device or about the device. For instance, a network receiving a request from a device may store geolocation information about a device. For example, to generate the score, the Accused Instrumentalities use information including one or more user-added hardware identifiers, such as a mobile identification number (“MIN”) or any derivation of a MIN or any related number; mobile subscription identification number (“MSIN”); an international mobile subscriber identity (“IMSI”) or encrypted version thereof (“TMSI”); Subscriber Module (SIM) Card serial number; serial number, Host Device ID, or any other unique identifier for a device (including but not limited to Android ID, UDID, IDFA, AAID) that is associated with the geolocation information disclosed below: <i>See, e.g.,</i> RQ-ATT0000070-RQ-ATT0000086 (https://about.att.com/privacy/privacy-notice.html).
--	---

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

	The information we collect x To better run our business, we collect information about you, your equipment and how you use our products and services. This can include: • Account information. You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including Customer Proprietary Network Information. • Equipment information. We collect information about equipment on our network like the type of device you use, device ID, and phone number. • Network performance. We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working. • Location information. Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites. • Web browsing and app information. We automatically collect a variety of information which may include time spent on websites or apps, website and IP addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information. • Biometric information. Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our Biometric Information Privacy Notice. • Third-party information. We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T. An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 14. The system recited in claim 12 wherein the device fingerprint is determined based at least in part on at least one of a	Within the Accused Instrumentalities the device fingerprint is determined based at least in part on at least one of a set of device settings, a set of installed applications, an indication of a software version, and a contact list.

set of device settings, a set of installed applications, an indication of a software version, and a contact list.	For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/). How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req’s compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req’s apply. Details at att.com/activearmorapp. <i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the device fingerprint is determined based at least in part on at least one of a set of device settings, a set of installed applications, an indication of a software version, and/or a contact list.
--	---

See ATT-RQ_0000042, -43, -44 (evidencing fingerprint information such device specific data, device settings, installed applications (e.g., ActiveArmor), system or application software versions (“Device OS”, “ActiveArmor Version Information”), contact list data (TN from Device Address Book), or other data specific to the calling device is stored and shared with AT&T’s “Vendor/Partner Hiya”):

Active Armor Data Elements

As part of the Active Armor Robocall mitigation program, data elements related to calling are shared with our Vendor/Partner Hiya. Note that Hiya's usage and management of these data elements is under written agreement with AT&T.

AT&T GFMO (Global Fraud Management Office) and AT&T CDO (Chief Data Office) each provide a set of per-Number data elements. AT&T CTS/PRS uses an API to provide per-Call data elements. There are additional data elements that are under investigation to determine if they will have value in Robocall Mitigation.

The following is a listing of each data element, by data source. See attached spreadsheet for more details.

AT&T CTS/PRS**Call Direction Response API (Per Call Basis)**

callEventNotification
 notificationType
 eventDescription
 correlationId
 callingParticipant
 callingParticipantName
 callingParticipantAlternate
 calledParticipant
 callingParticipantPrivacy
 callSessionIdentifier
 addressDirection:
 originatorTasId:
 callingParticipantAccessNetworkInfo
 callbackData
 link

 action
 actionToPerform
 displayName
 routingAddress
 decisionId
 displayAddress
 callInfo

	These are additional Parameters Call Direction Response API (CR 245) callInfoLocation callInfoPurpose callInfoType callInfoConfidence callInfoSource callInfoOrigin AT&T Account Services CTN (including AT&T/FN/Cricket customers) Service tier (like Basic vs. Advanced) Service Tags: • FirstNet • CRU • COU • Customers who have rate-plan-included Advanced service. • Cricket • Prepaid • Wireless Home Phone ActiveArmor Application Data TN from Device Address Book - Hashed (shared only with explicit subscriber consent) Device OS ActiveArmor Version Information
--	---

As another example, the device fingerprint is determined based at least in part on the installed ActiveArmor app, and/or the saved settings within said app. As another example, the device fingerprint is determined based at least in part on mobile identification number (“MIN”) or any derivation of a MIN or any related number; mobile subscription identification number (“MSIN”); an international mobile subscriber identity (“IMSI”) or encrypted version thereof (“TMSI”); Subscriber Module (SIM) Card serial number; serial number, Host Device ID, or any other unique identifier for a device (including but not limited to Android ID, UDID, IDFA, AAID), and/or the collected information set forth below, or any combination thereof.

See, e.g., RQ-ATT0000070-RQ-ATT0000086 (<https://about.att.com/privacy/privacy-notice.html>).

The information we collect

x

To better run our business, we collect information about you, your equipment and how you use our products and services. This can include:

- **Account information.** You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including [Customer Proprietary Network Information](#).
- **Equipment information.** We collect information about equipment on our network like the type of device you use, device ID, and phone number.
- **Network performance.** We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working.
- **Location information.** Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites.
- **Web browsing and app information.** We automatically collect a variety of information which may include time spent on websites or apps, website and IP addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information.
- **Biometric information.** Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our [Biometric Information Privacy Notice](#).
- **Third-party information.** We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T.

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

	How we use your information x We rely on the information we collect to support our business functions, power our services and improve your experience, such as when we: • Combine it with the information from testing and running our network to determine which products and services better meet the needs of our customers. • Provide our products and services. • Contact you. • Improve your experience and safety. This includes verifying your identity, detecting and preventing fraud, protecting your financial accounts, authorizing transactions and assisting your interactions with customer care. • Improve and protect our network. • Use it to help understand which additional products and services may interest you and others. (We don't access or use the content of your texts, emails or calls for this or any other marketing and advertising.) • Design and deliver advertising, marketing and promotional campaigns to you and others – and measuring their effectiveness (See your choices). • Use it for billing, collection, and protection of our property and legal rights. • Prevent and investigate security issues, illegal activities, and violations of our terms and conditions. • Conduct research and create aggregated reports – reports that offer insights about groups of customers, but not individuals (we do not attempt to re-identify individuals in aggregated reports). <i>See also</i> RQ-ATT0000139-RQ-ATT0000150 (https://www.att.com/legal/terms.activeArmorMobileSecurity.html):
--	--

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

	In order to perform the functions of the Service including but not limited to its Call Features, AT&T may use and/or disclose or allow the disclosure to our third-party vendor(s) of Your personal information, including without limitation mobile number, contacts/address book in order to populate detail in the call detail screen, the presence or absence of calling party phone numbers in your Device address book, and App usage information, such as which numbers you report and/or manually block within the App, as factors to determine which callers are suspected fraud and spam. The contact names and phone numbers in your Device address book are not shared for any purpose other than improving your experience with the App by helping you to recognize known callers. 3.2 Consent for Information Disclosure in Connection with Data Features The Service includes the following data security and related features: Device Security Alerts, Data Breach Alerts, Public Wi-Fi Protection (VPN & Wi-Fi Alerts), Identity Monitoring, Reverse Number Lookup, Safe Browsing, and Device Theft Alerts (collectively “Data Features”) In order to perform the functions and to improve the effectiveness of the Service including but not limited to its Data Features for all users, AT&T, its pertinent suppliers and their subsidiaries, agents and subcontractors may collect, maintain, process, use, and disclose diagnostic, technical, usage and related information including, but not limited to, information about: • the type of Device You are using and the operating system You are running; • Your applicable wireless network provider/carrier; • the applications and files present on Your Device and SD memory card; • the results of any scans performed by the App; and • actions You take as a result of any virus or malware notifications. We also may collect information about how the App and any associated Service applications behave on Your Device and the network services with which applications installed on Your Device communicate in order to determine if any applications are behaving maliciously (for example, is an application accessing Your address contacts, sending premium-rate text messages that charge money to Your wireless bill, or communicating with a server known to host phishing websites). An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 15. The system recited in claim 12 wherein the user-added hardware identifier is associated with a memory card.	Within the Accused Instrumentalities wherein the user-added hardware identifier is associated with a memory card. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.”

See, e.g., RQ-ATT0000035-RQ-ATT0000041 (<https://www.att.com/security/>).

How do AT&T and the other major carriers differ in terms of security? ^

AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.

To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost.

ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited

Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp.

Feedback



See also RQ-ATT0000012-RQ-ATT0000023 (<https://sustainability.att.com/priority-topics/network-data-security>).

As one example, the user-added hardware identifier is associated with a memory card. As another example, the user-added hardware identifier is associated with a SIM card in the calling device. See, e.g., RQ0002042-RQ0002060 (https://en.wikipedia.org/wiki/SIM_card).

	An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 16. The system recited in claim 1 wherein the one or more processors are configured to confirm an observed phone number associated with the call.	Within the Accused Instrumentalities the one or more processors are configured to confirm an observed phone number associated with the call. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/). How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req’s compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req’s apply. Details at att.com/activearmorapp.

	<i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the one or more processors are configured to confirm an observed phone number associated with the call, such as the phone number of the calling party and/or such as the phone number in the SIP INVITE. An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 17. The system recited in claim 1 wherein the information associated with the call is provided by an agent on the calling device.	Within the Accused Instrumentalities the information associated with the call is provided by an agent on the calling device. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. <i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the information associated with the call is provided by an agent on the calling device, including but not limited to a mobile application such as the ActiveArmor app. As yet another example, the agent is artificial intelligence that generates the SIP INVITE. An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation
--	--

	and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 18. The system recited in claim 1 wherein the information associated with the call is provided in response to one of a detection of an outgoing communication and a prompt to validate communication session information.	Within the Accused Instrumentalities the information associated with the call is provided in response to one of a detection of an outgoing communication and a prompt to validate communication session information. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” See, e.g., RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/). How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req’s compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req’s apply. Details at att.com/activearmorapp.

	<i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the information associated with the call, such as SIP headers that are transmitted, is provided in response to one of a detection of an outgoing communication and a prompt to validate communication session information, such as an outgoing call and a SIP INVITE. An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 19. The system recited in claim 1 wherein the score is based at least in part on an age of the information associated with the calling device.	Within the Accused Instrumentalities the score is based at least in part on an age of the information associated with the calling device. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. Feedback See also RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the score, or the attestation level, is based at least in part on an age of the information associated with the calling device, such as an age of the information provided in the SIP INVITE and/or the age of the SIP INVITE, including but not limited to timing parameters such as a timestamp, the “iat” attribute, a counter, a nonce, Invite request retransmit interval, Invite transaction timeout timer, and/or any other SIP invitation timing parameter. See, e.g., RQ0001945-RQ0001948 (https://www.carrierx.com/documentation/how-it-works/stir-shaken#sip-identity-header).
--	---

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

	An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 20. The system recited in claim 1 wherein the score is based at least in part on one or more of feedback associated with a particular phone call, an indication of a stolen device, an indication of a potential spoof attempt, an indication of fraud related to a device, or an indication of a verification that was subsequently determined to be errant.	Within the Accused Instrumentalities the score is based at least in part on one or more of feedback associated with a particular phone call, an indication of a stolen device an indication of a potential spoof attempt, an indication of fraud related to a device, or an indication of a verification that was subsequently determined to be errant. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. <i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the score, including the attestation level, is based at least in part on one or more of feedback associated with a particular phone call, an indication of a stolen device an indication of a potential spoof attempt, an indication of fraud related to a device, or an indication of a verification that was subsequently determined to be errant. As another example, the score is based in part on feedback and/or indicators of a potential spoof, including prior indicators and/or labeling of a call as “spam,” “Telemarketer,” “potential fraud,” feedback from a user, prior complaints by callees,
--	---

	prior blocking requests by callees, prior history of brief call lengths, and/or prior history of less telephone calls. <i>See, e.g.,</i> RQ-ATT0000133-RQ-ATT0000134 (https://www.att.com/support/pages/report-call-or-text). Report unwanted calls & texts AT&T ActiveArmor™ works 24/7 to help stop threats before they get to you. Unwanted calls and texts are annoying, and some could be fraudulent or illegal. Report offenders that slip through and help block them! • Forward suspicious messages to 7726 (SPAM). • Complete the form to help block spam, robocalls, and unwanted text messages. • Download AT&T Call Protect on your phone to manage future unwanted callers. An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 21. The system recited in claim 1 wherein the score comprises a reputation score.	Within the Accused Instrumentalities the score comprises a reputation score. As one example, the score generated for the calling device that contains a reputation score may be from Defendants, a third party (e.g. Hiya), or some combination thereof. As another example, Enterprise Caller Scoring is a score generated for the calling device that indicates the validity of a phone number. <i>See, e.g.,</i> https://www.hiya.com/products/enterprise-caller-scoring:

How it Works

Enterprise Caller Scoring is a new layer of Hiya's Adaptive AI that stops number rotation — the practice of switching phone numbers to avoid spam detection — from being effective on mobile networks.

Like a credit agency for enterprise callers, Enterprise Caller Scoring assesses incoming calls based on the calling enterprise's history across all the numbers they own. It can identify the calling enterprise's reputation for more than 150 million enterprise phone numbers in the US — even phone numbers that haven't yet built a calling history. An enterprise's reputation continuously evolves based on behavior and is automatically recognized across all their numbers.

See also <https://blog.hiya.com/how-hiyas-proprietary-adaptive-ai-stops-phone-spam>.

For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (<https://www.att.com/security/>).

How do AT&T and the other major carriers differ in terms of security? ^

AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.

To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost.

ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited

Req’s compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req’s apply. Details at att.com/activearmorapp.

Feedback

CHAT

See also RQ-ATT0000012-RQ-ATT0000023 (<https://sustainability.att.com/priority-topics/network-data-security>).

As one example, the score comprises a reputation score. As another example, the score is the attestation level and the attestation level comprises a reputation score. As another example, the score

	comprises a reputation score based on data collected by AT&T, including the following: <i>See, e.g.</i>, RQ-ATT0000070-RQ-ATT0000086 (https://about.att.com/privacy/privacy-notice.html). The information we collect x To better run our business, we collect information about you, your equipment and how you use our products and services. This can include: • Account information. You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including Customer Proprietary Network Information. • Equipment information. We collect information about equipment on our network like the type of device you use, device ID, and phone number. • Network performance. We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working. • Location information. Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites. • Web browsing and app information. We automatically collect a variety of information which may include time spent on websites or apps, website and IP addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information. • Biometric information. Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our Biometric Information Privacy Notice. • Third-party information. We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T.
--	---

	How we use your information x We rely on the information we collect to support our business functions, power our services and improve your experience, such as when we: • Combine it with the information from testing and running our network to determine which products and services better meet the needs of our customers. • Provide our products and services. • Contact you. • Improve your experience and safety. This includes verifying your identity, detecting and preventing fraud, protecting your financial accounts, authorizing transactions and assisting your interactions with customer care. • Improve and protect our network. • Use it to help understand which additional products and services may interest you and others. (We don’t access or use the content of your texts, emails or calls for this or any other marketing and advertising.) • Design and deliver advertising, marketing and promotional campaigns to you and others – and measuring their effectiveness (See your choices). • Use it for billing, collection, and protection of our property and legal rights. • Prevent and investigate security issues, illegal activities, and violations of our terms and conditions. • Conduct research and create aggregated reports – reports that offer insights about groups of customers, but not individuals (we do not attempt to re-identify individuals in aggregated reports). <i>See also</i> RQ-ATT0000139-RQ-ATT0000150 https://www.att.com/legal/terms.activeArmorMobileSecurity.html):
--	---

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

	In order to perform the functions of the Service including but not limited to its Call Features, AT&T may use and/or disclose or allow the disclosure to our third-party vendor(s) of Your personal information, including without limitation mobile number, contacts/address book in order to populate detail in the call detail screen, the presence or absence of calling party phone numbers in your Device address book, and App usage information, such as which numbers you report and/or manually block within the App, as factors to determine which callers are suspected fraud and spam. The contact names and phone numbers in your Device address book are not shared for any purpose other than improving your experience with the App by helping you to recognize known callers. 3.2 Consent for Information Disclosure in Connection with Data Features The Service includes the following data security and related features: Device Security Alerts, Data Breach Alerts, Public Wi-Fi Protection (VPN & Wi-Fi Alerts), Identity Monitoring, Reverse Number Lookup, Safe Browsing, and Device Theft Alerts (collectively “Data Features”) In order to perform the functions and to improve the effectiveness of the Service including but not limited to its Data Features for all users, AT&T, its pertinent suppliers and their subsidiaries, agents and subcontractors may collect, maintain, process, use, and disclose diagnostic, technical, usage and related information including, but not limited to, information about: • the type of Device You are using and the operating system You are running; • Your applicable wireless network provider/carrier; • the applications and files present on Your Device and SD memory card; • the results of any scans performed by the App; and • actions You take as a result of any virus or malware notifications. We also may collect information about how the App and any associated Service applications behave on Your Device and the network services with which applications installed on Your Device communicate in order to determine if any applications are behaving maliciously (for example, is an application accessing Your address contacts, sending premium-rate text messages that charge money to Your wireless bill, or communicating with a server known to host phishing websites). An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 22. The system recited in claim 1 wherein the value is generated at least in part by the calling device.	Within the Accused Instrumentalities the value is generated at least in part by the calling device. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” See, e.g., RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

How do AT&T and the other major carriers differ in terms of security?

AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.

To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost.

ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited

Req’s compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req’s apply. Details at att.com/activearmorapp.

 Feedback 

 CHAT

See also RQ-ATT0000012-RQ-ATT0000023 (<https://sustainability.att.com/priority-topics/network-data-security>).

As one example, the value is generated at least in part by the calling device. For example, the SIP Identity header is generated at least in part by the calling device itself. See, e.g., RQ0001970 (<https://sti-ga.atis.org/resources/>). As yet another example, the SIP Identity header comprises the Personal Assertion Token (PASSporT), which is a value generated at least in part by the calling device. See, e.g., RQ0001970 (<https://sti-ga.atis.org/resources/>).

For example, the value generated based at least in part on information associated with the calling device can include a device fingerprint, device information (e.g., make, model, serial number, operating system version, application information, or other identifying information of a device), customer account information, location information, caller or callee number, or other information associated with the device and upon which (or upon verification of which) a security determination is in part based. The value generated based at least in part on information associated with the calling device may be generated from Defendants, a third party (e.g., Hiya), or some combination thereof.

As another example, the following device specific information (e.g., settings, software versions, contact list data, and other data specific to the calling device) represents a value generated at least in part by the calling device. *See* ATT-RQ_0000042, -43, -44 (evidencing information such device specific data, device settings, installed applications (e.g., ActiveArmor), system or application software versions (“Device OS”, “ActiveArmor Version Information”), contact list data (TN from Device Address Book), or other data specific to the calling device is stored and shared with AT&T’s “Vendor/Partner Hiya”):

Active Armor Data Elements

As part of the Active Armor Robocall mitigation program, data elements related to calling are shared with our Vendor/Partner Hiya. Note that Hiya’s usage and management of these data elements is under written agreement with AT&T.

AT&T GFMO (Global Fraud Management Office) and AT&T CDO (Chief Data Office) each provide a set of per-Number data elements. AT&T CTS/PRS uses an API to provide per-Call data elements. There are additional data elements that are under investigation to determine if they will have value in Robocall Mitigation.

The following is a listing of each data element, by data source. See attached spreadsheet for more details.

AT&T CTS/PRS**Call Direction Response API (Per Call Basis)**

callEventNotification
notificationType
eventDescription
correlationId
callingParticipant
callingParticipantName
callingParticipantAlternate
calledParticipant
callingParticipantPrivacy
callSessionIdentifier
addressDirection:
originatorTasId:
callingParticipantAccessNetworkInfo
callbackData
link

action
actionToPerform
displayName
routingAddress
decisionId
displayAddress
callInfo

	These are additional Parameters Call Direction Response API (CR 245) callInfoLocation callInfoPurpose callInfoType callInfoConfidence callInfoSource callInfoOrigin AT&T Account Services CTN (including AT&T/FN/Cricket customers) Service tier (like Basic vs. Advanced) Service Tags: • FirstNet • CRU • COU • Customers who have rate-plan-included Advanced service. • Cricket • Prepaid • Wireless Home Phone ActiveArmor Application Data TN from Device Address Book - Hashed (shared only with explicit subscriber consent) Device OS ActiveArmor Version Information
--	---

	An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 23. The system recited in claim 1 wherein the value is provided at least in part by an entity different from the calling device.	Within the Accused Instrumentalities the value is provided at least in part by an entity different from the calling device. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/). How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req’s compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req’s apply. Details at att.com/activearmorapp.

	<i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As another example, the value is provided by Defendants and/or at Defendants’ direction and/or control by a third-party entity (e.g. Hiya) that is different from the calling device. As one example, the value is provided at least in part by an entity different from the calling device. As another example, the SIP Identity header is provided at least in part by an entity different from the calling device, such as by the Accused Instrumentalities. See, e.g., RQ0001970 (https://stiga.atis.org/resources/). As another example, the SIP Identity header comprises the Personal Assertion Token (PASSporT), which is a value provided at least in part by an entity different from the calling device, such as by the Accused Instrumentalities. See, e.g., RQ0001970 (https://stiga.atis.org/resources/). An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff
Claim 24. The system recited in claim 1 wherein the value comprises at least one of an authentication code, a counter value, a pseudo-random number, a number specific to a particular session, or a number specific to the calling device.	Within the Accused Instrumentalities the value comprises at least one of an authentication code, a counter value, a pseudo-random number, a number specific to a particular session, or a number specific to the calling device. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” See, e.g., RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. <i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the value comprises at least one of an authentication code, a counter value, a pseudo-random number, a number specific to a particular session, and/or a number specific to the calling device. As another example, the SIP Identity header comprises at least one of an authentication code, a counter value, a pseudo-random number, a number specific to a particular session, and/or a number specific to the calling device. <i>See, e.g.,</i> RQ0002102-RQ0002103 (https://www.carrierx.com/documentation/how-it-works/stir-shaken-how-stirshaken-works)
--	---

	An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 25. The system recited in claim 1 wherein the security determination is performed based at least in part on evaluate of the score against a threshold score.	Within the Accused Instrumentalities the security determination is performed based at least in part on evaluate of the score against a threshold score. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/). How do AT&T and the other major carriers differ in terms of security? AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req’s compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req’s apply. Details at att.com/activearmorapp.

	See also RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the security determination is performed based at least in part on evaluate of the score against a threshold score. As another example, the security determination is performed based at least in part on evaluate of the attestation level against a threshold attestation level. 5.2.3 Attestation Indicator (“attest”) <u>The “attest” claim allows the originating service provider that is populating an Identity header to clearly indicate the information it can vouch for regarding the origination of the call.</u> ~~This indicator allows for both identifying the service provider that is vouching for the call as well as clearly indicating what information the service provider is attesting to.~~ In the SHAKEN framework we define the following three levels of attestation: A. Full Attestation: The signing provider shall satisfy all of the following conditions: • Is responsible for the origination of the call onto the IP-based service provider voice network. • Has a direct authenticated relationship with the customer and can identify the customer. • Has established a verified association with the telephone number used for the call. NOTE 1: The signing provider is asserting that their customer can “legitimately” use the number that appears as the calling party (i.e., the Caller ID). The legitimacy of the telephone number(s) the originator of the call can use is subject to signer-specific policy, but could use mechanisms such as the following: • The number was assigned to this customer by the signing service provider. • This number is one of a range of numbers assigned to an enterprise or wholesale customer. • The signing service provider has ascertained that the customer is authorized to use a number (e.g., by business agreement or evidence the customer has access to use the number). This includes numbers assigned by another service provider. • The number is not permanently assigned to an individual customer but the signing provider can track the use of the number by a customer for certain calls or during a certain timeframe. NOTE 2: Ultimately it is up to service provider policy to decide what constitutes “legitimate right to assert a telephone number” but the service provider’s reputation may be directly dependent on how rigorous they have been in making this assertion.
--	--

	B. Partial Attestation: The signing provider shall satisfy all of the following conditions: • Is responsible for the origination of the call onto ~~its-the~~ IP-based <u>service provider</u> voice network. • Has a direct authenticated relationship with the customer and can identify the customer. • Has NOT established a verified association with the telephone number being used for the call. 9 ATIS-1000074-E -- SIP Forum TWG-10-E <u>NOTE: By populating this value, the service provider attests that it can trace the source of the call to a customer for policy enforcement purposes</u>~~When partial attestation is used, each customer will have a unique origination identifier created and managed by the service provider, but the intention is that it will not be possible to reverse engineer the identity of the customer purely from the identifier or signature. As described in section 5.2.4, the unique origination identifier allows data analytics to establish a reputation profile and assess the reliability of information asserted by the customer assigned this unique identifier. The identifier also provides a reliable mechanism to determine the customer for forensic analysis or legal action where appropriate.~~ <i>See, e.g.,</i> RQ0001970 (https://sti-ga.atis.org/resources/). An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 26. The system recited in claim 1 wherein the score is based at least in part on an age of a timestamp.	Within the Accused Instrumentalities the score is based at least in part on an age of a timestamp. For example, AT&T advertises: “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g.,</i> RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. <i>See also</i> RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the score is based at least in part on an age of a timestamp. As another example, the attestation level is based, at least in part, on the age of the timestamp in the SIP INVITE. As another example, the SIP INVITE various timing parameters upon which the score, including the attestation level is based at least in part, including but not limited to a timestamp, counter, nonce, Invite request retransmit interval, Invite transaction timeout timer, or any other SIP invitation timing parameters, and the one or more processors of the Accused Instrumentalities are configured to
--	---

	prevent a replay attack using the timestamp. <i>See, e.g.</i>, RFC 8224 (directing that a PASSporT for a SIP request “MUST NOT [be] generated . . . if the Date header is outside of its local policy for freshness (sixty seconds is RECOMMENDED”). An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 27. [pre] A method, comprising:	This is the preamble of the claim and is not limiting. To the extent the preamble is construed as limiting, the Accused Instrumentalities comprise a method(s) that performs the limitations of the claim. The Accused Instrumentalities, alone and/or in combination, comprise one or more method(s) and service(s) that determine if a given call should transmit a notification directed to the callee device, based upon a security determination that utilizes a cryptographic element associated with the caller device, and/or detect, block, and prevent SPAM, fraudulent, and spoofed phone calls. <i>See, e.g.</i>, RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security):

- **Robocall Scam Identification & Mitigation:** AT&T has established mechanisms to identify illegal robocall campaigns and help to mitigate them.
 - Through the complementary programs listed below, [AT&T has blocked or labeled billions of unwanted robocalls](#).
 - [AT&T ActiveArmorSM](#) automatically blocks fraud calls and labels other suspected spam calls so a wireless customer can choose to answer or not. It identifies the calls through data analytics, network intelligence and customer reports.
 - AT&T’s Global Fraud Management team works closely with the U.S. Telecom Industry [Traceback Group](#) and law enforcement to identify the source of illegal calls. This process provides necessary information to stop illegal robocall campaigns and places responsibility on service providers for traffic that originates on their networks.
 - AT&T’s Global Fraud Management organization, with assistance from the AT&T Chief Data Office, uses sophisticated algorithms to examine billions of calls each day for patterns that indicate a robocalling scheme. They investigate suspicious activity that may be illegal, relying on human fraud expertise before blocking.
 - Implementation of the caller ID authentication standard known as [STIR/SHAKEN](#) remains a top priority for AT&T, and we have deployed it across our IP networks. We have filed comments with the Federal Communications Commission (FCC) detailing our progress on this front and offering our support as the FCC addresses the complex details of implementation. We also supported the TRACED Act, which codified implementation requirements.

For example, AT&T advertises “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” See, e.g., RQ-ATT0000035-RQ-ATT0000041 (<https://www.att.com/security/>).

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. As another example, AT&T advertises that with Digital Phone Call Protect, customers get “call validation,” “Automatic fraud blocking,” and “Suspected spam call warning,” among other features. See, e.g., RQ-ATT0000137-RQ-ATT0000138 (https://www.att.com/support/article/u-verse-voice/KM1235421/)
--	--

Digital Phone Call Protect features

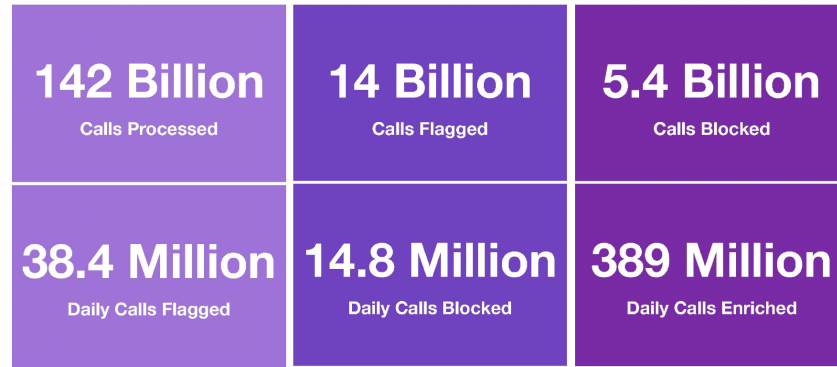
Here's what you get with Digital Phone Call Protect¹:

- **Call validation:** Soon you'll see a [V] on your caller ID for some calls. This means we've confirmed that the call originated from the phone registered to that number. (Remember to still be cautious when answering a call from an unknown number.)
- **Automatic fraud blocking:** Each potential fraud call gives the caller a busy signal, and the call won't go through. You can toggle this feature on or off.
- **Call blocking:** If you have a specific number you want to block, press *61 after the unwanted call to block that number.
- **Call log:** You can see detailed call log info.
- **Suspected spam call warning:** Your caller ID will show Suspected Spam and a type (Political, Nonprofit, Telemarketer, Survey, or Robocaller).

For example, the Accused Instrumentalities comprises one or more processors configured to implement protocols, technologies, features, and services for validating and/or verifying caller identification information including without limitation STIR/SHAKEN.

See, e.g., ATT-RQ_0000001 at 3 (showing volume of blocks calls necessitating the use of computer systems with processors to make the determination to block or connect an outgoing or incoming call):

Hiya-AT&T Call Protect 2023 Summary



3 | HIYA PROPRIETARY AND CONFIDENTIAL

hiya

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

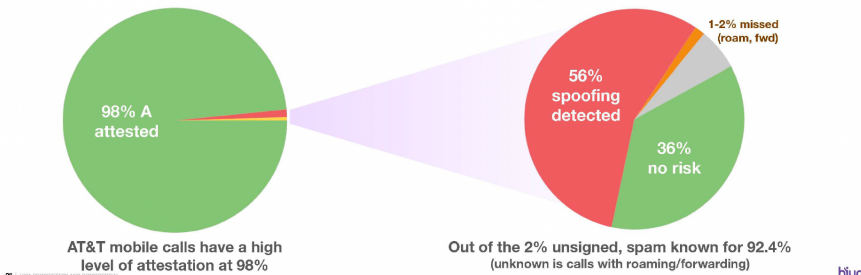
ATT-RQ_0000003

See, e.g., ATT-RQ_0000001 at 26 (showing that AT&T prevents spoofing from its own numbers on its network):

Working with AT&T, Hiya has been successful at preventing spoofing from AT&T phone numbers

STATE OF THE SERVICE TODAY:

Working closely with AT&T, Hiya has solutions in place to address the challenges in mobile spoof detection. Hiya has deployed in production a mobile spoof detection solution that we feel is detecting **98% of spoofed calls using AT&T mobile numbers**, and detecting a large majority of spoofing using other mobile carrier lines.



20 | HIYA PROPRIETARY AND CONFIDENTIAL

hiya

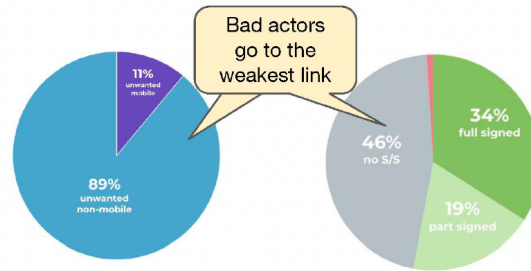
RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

ATT-RQ_0000026

See, e.g., ATT-RQ_0000001 at 28 (noting that call authentication technologies beyond

STIR/SHAKEN are required to prevent fraudulent, spam, and spoofed phone calls):

However, the majority of unwanted calls stem from non-mobile sources, and STIR/SHAKEN is far from fixing this issue



89% of unwanted calls are non-mobile originated

with 66% of calls not fully signed

STATE OF THE ECOSYSTEM:

Key impediments on STIR/SHAKEN non-mobile spoofing include:

- Unstable Implementation for Non-Mobile Numbers
- Challenges from Legacy Systems
- Incomplete Adoption Among Service Providers
- Verification and Trust Issues

These complexities provide opportunities for scammers to exploit coverage gaps

Calls from non-mobile sources are much more likely to be unwanted compared to calls from mobile sources

28 | HIXA PROPRIETARY AND CONFIDENTIAL

hiya

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

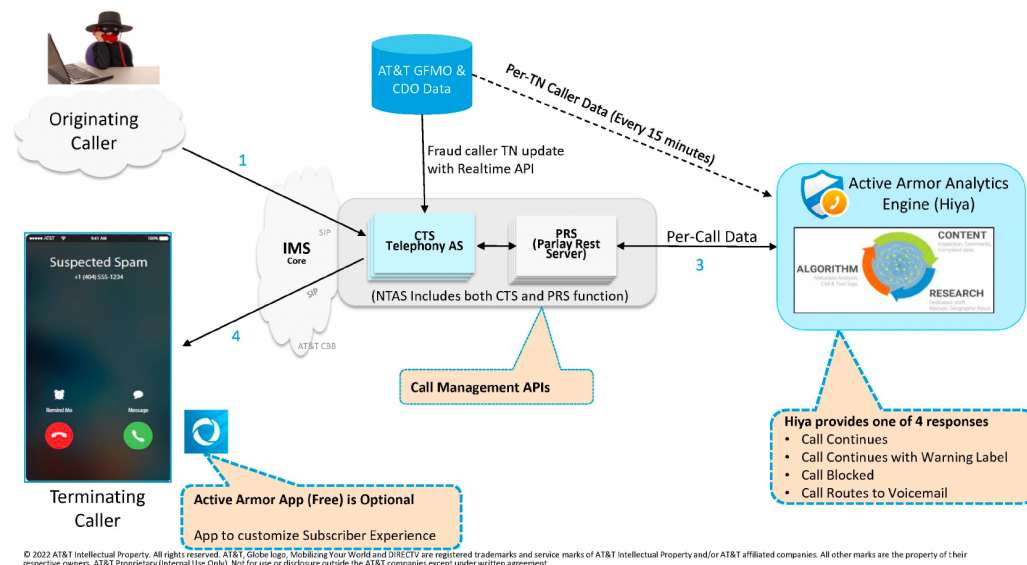
ATT-RQ_0000028

The Accused Instrumentalities are implemented, used, and/or put into service by AT&T in intra- and inter- network communications. See, e.g., RQ-ATT0000051-RQ-ATT0000053 (https://about.att.com/story/2019/att_tmo_call-authentication.html).

	AT&T* and T-Mobile today began rollout of cross-network call authentication based on SHAKEN/STIR standards – another big step toward protecting consumers from unwanted robocalls. SHAKEN/STIR technology lets consumers know that an incoming call is really coming from the number listed on the caller ID display – not a spoofed robocall or scammer. While authentication won’t solve the problem of unwanted robocalls by itself, it is a key step toward giving customers greater confidence and control over the calls they answer. For example, a call that is illegally “spoofed” – or shows a faked number – will fail the SHAKEN/STIR Caller ID verification and will not be marked as verified. By contrast, verification will confirm that a call is really coming from the identified number or entity. More calls will be verified over time as more device providers participate, and as more network providers implement the standards. The FCC has recommended SHAKEN/STIR standards to digitally validate phone calls. The acronym stands for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR). For more information on all the ways AT&T is protecting customers, visit https://about.att.com/story/2019/att_call_protect.html and https://att.com/CyberAware.
--	---

See, e.g., ATT-RQ_0000045 (Hiya provides at least one of four responses – namely, “Call Continues,” “Call Continues with Warning Label”, “Call Blocked” or “Call Routes to Voicemail” (e.g., whether or not the call has an assurance or a failure of an assurance)):

AT&T Active Armor (Call Protect) – High Level Architecture



RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

ATT-RQ_0000045

As another example, the Accused Instrumentalities implement STIR/SHAKEN, among other protocols, technologies, features, and services for validating and/or verifying caller identification information. See, e.g., RQ-ATT0000024-RQ-ATT0000026 (https://about.att.com/story/2019/call_validation_displays.html):

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

	AT&T* has turned on its first phone displays that let you know an incoming call is really from the number appearing on Caller ID. This fights against “spoofing” of phone numbers – a trick used by many illegal robocallers. Most AT&T customers with a Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ™ will see a special display when an incoming call has been authenticated. They will see a green checkmark and the words, “Valid Number.” Consumers with AT&T Phone digital home phone service also can activate the feature. It will give them a “[V]” for valid number. Phone service providers have jointly developed a technology – the SHAKEN/STIR standards – to digitally validate calls. This won’t solve the problem of unwanted robocalls by itself. But it can give consumers greater confidence and control over the calls they answer. “This is another step to tame annoying, unwanted robocalls,” said Kevin Petersen, AT&T senior vice president, Postpaid Wireless Products. “In the coming year, we’ll continue to take more steps and put more pressure on the bad guys.” AT&T is rolling out its SHAKEN/STIR display as part of its AT&T Call Protect service, which is being added at no charge to millions of mobility consumer lines. AT&T Call Protect blocks or labels suspected illegal and unwanted robocalls. This strategy will give a multiplier effect to call protection: A “valid number” on an AT&T device means the incoming call has been authenticated by SHAKEN/STIR <i>and</i> passed through AT&T Call Protect screening.
--	---

Here are some other key points:

- A call that shows “valid number” has been verified and can increase your trust level. But a call without the label may still be a legitimate call. More calls will be marked with “valid number” over time, as more network providers implement SHAKEN/STIR and link to each other.
- AT&T has rolled out AT&T Call Protect automatically to many Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ users. Others are on the way soon.¹ If you’re not seeing call validation on those devices when you accept their latest software update, you don’t have to wait. You can download the AT&T Call Protect app, or turn on the service from your account settings in myAT&T.
- AT&T Phone digital home phone users can opt-in to get AT&T Digital Phone Call Protect and call validation. Just go to your account settings on myAT&T and turn it on.
- Validation displays will be added to more mobile devices in the new year.
- Finally, a “valid number” display helps fight against bad guys, but it can never guarantee an individual caller is a good guy. Consumers should always use their best judgement when answering calls from strangers.

See, e.g., RQ-ATT0000051-RQ-ATT0000053 (https://about.att.com/story/2019/att_tmo_call_authentication.html).

AT&T* and T-Mobile today began rollout of cross-network call authentication based on SHAKEN/STIR standards – another big step toward protecting consumers from unwanted robocalls.

SHAKEN/STIR technology lets consumers know that an incoming call is really coming from the number listed on the caller ID display – not a spoofed robocall or scammer. While authentication won’t solve the problem of unwanted robocalls by itself, it is a key step toward giving customers greater confidence and control over the calls they answer.

For example, a call that is illegally “spoofed” – or shows a faked number – will fail the SHAKEN/STIR Caller ID verification and will not be marked as verified. By contrast, verification will confirm that a call is really coming from the identified number or entity. More calls will be verified over time as more device providers participate, and as more network providers implement the standards.

The FCC has recommended SHAKEN/STIR standards to digitally validate phone calls. The acronym stands for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR).

For more information on all the ways AT&T is protecting customers, visit https://about.att.com/story/2019/att_call_protect.html and <https://att.com/CyberAware>.

Caller identification authentication and verification technology, including without limitation, STIR/SHAKEN is a technology to detect spoofed phone calls, using one or more processors. *See, e.g.*, RQ0001970 (<https://sti-ga.atis.org/resources/>).

	ATIS STANDARD ATIS-1000074-E -- SIP Forum TWG-10-E
	ATIS Standard on – Signature-based Handling of Asserted information using toKENs (SHAKEN) 1 Scope & Purpose 1.1 Scope This document is intended to provide telephone service providers with a framework and guidance on how to utilize Secure Telephone Identity (STI) technologies toward the validation of legitimate calls and the mitigation of illegitimate spoofing of telephone identities on IP-based service provider voice networks (also to be referred to as Voice over Internet Protocol [VoIP] networks). The primary focus of this document is on the format of STI claims, the mapping of these claims to SIP (RFC 3261), and the authentication and verification functions. 1.2 Purpose Using the protocols defined in ~~draft-ietf-stir-rfc4474bis~~RFC 8224 and ~~draft-ietf-stir-passport~~RFC 8225, this document defines the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework. This framework is targeted at telephone service providers delivering phone calls over VoIP, and addresses the implementation and usage of the IETF STIR Working Group protocols and the architecture and use of STI-related X.509-based certificates (RFC 5280). It also discusses the general architecture of service provider authentication and verification services. Finally, it provides high level guidance on the use of positive or negative verification of the signature to mitigate illegitimate telephone identity in general. Illegitimate Caller ID spoofing is a growing concern for North American telephone service providers and their customers. There are many Caller ID spoofing mechanisms, and illegitimate spoofing can evolve to evade mitigation techniques. Service provider solutions must therefore be flexible to respond to evolving threats in much the same way as cybersecurity solutions. In addition, the integration of new technologies into established VoIP networks imposes many interoperability and interworking challenges. As a result, this document is a baseline document on the implementation of the protocol-related requirements for STI. The objective is to provide a baseline that can evolve over time, incorporating more comprehensive functionality and a broader scope in a backward compatible and forward looking manner.
27[a] receiving information pertaining to a call initiated by a	The Accused Instrumentalities receive information pertaining to a call initiated by a calling device, the information pertaining to the call including: (1) a value generated based at least in part on

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

calling device, the information pertaining to the call including: (1) a value generated based at least in part on information associated with the calling device, and (2) a score generated for the calling device, the score indicating a validity of a phone number;	information associated with the calling device, and (2) a score generated for the calling device, the score indicating a validity of a phone number. For example, the value generated based at least in part on information associated with the calling device can include a device fingerprint, device information (e.g., make, model, serial number, operating system version, application information, or other identifying information of a device), customer account information, location information, or other information associated with the device. Furthermore, the score, which is generated for the calling device, indicates a validity of the phone number and is used to convey assurance or failure to confirm to the callee associated with the call. As one example, the received information pertaining to the call includes a score generated for the calling device, the score indicating a validity of a phone number. The score generated for the calling device may be scored from Defendants, a third party (e.g. Hiya), or some combination thereof. The score can be generated by one or more machine learning algorithms. <i>See e.g.</i>, https://work.hiya.com/adaptive-ai-ebook
---	--

Adaptive AI: A Proactive Strategy for Stopping Scam and Fraud Calls

Adaptive AI is an innovative new feature of Hiya Protect, a proprietary call protection service used by carriers, distribution partners and the Hiya mobile app.

Unlike other capabilities on the market today, Adaptive AI uses machine learning to proactively hunt and shut down scam campaigns. With the ability to stay ahead of scammers, Adaptive AI works in real-time, without the need for human intervention or any updating of existing AI models.

For example, the value generated based at least in part on information associated with the calling device can include a device fingerprint, device information (e.g., make, model, serial number, operating system version, application information, or other identifying information of a device), customer account information, location information, caller or callee number, or other information associated with the device and upon which (or upon verification of which) a security determination is in part based. The value generated based at least in part on information associated with the calling device may be generated from Defendants, a third party (e.g., Hiya), or some combination thereof. *See* ATT-RQ_0000042, -43, -44 (evidencing device specific data, device settings, installed applications e.g., ActiveArmor, system or application software versions (e.g., “Device OS”, “ActiveArmor Version Information”), contact list data (TN from Device Address Book), or other data associated with the calling device is stored and shared with AT&T’s “Vendor/Partner Hiya”). These values are used to generate a score to indicate a validity of a phone number. That score is

used in the process of conveying assurance or failure to confirm for intra- and inter- network calls.

Active Armor Data Elements

As part of the Active Armor Robocall mitigation program, data elements related to calling are shared with our Vendor/Partner Hiya. Note that Hiya’s usage and management of these data elements is under written agreement with AT&T.

AT&T GFMO (Global Fraud Management Office) and AT&T CDO (Chief Data Office) each provide a set of per-Number data elements. AT&T CTS/PRS uses an API to provide per-Call data elements. There are additional data elements that are under investigation to determine if they will have value in Robocall Mitigation.

The following is a listing of each data element, by data source. See attached spreadsheet for more details.

AT&T CTS/PRS**Call Direction Response API (Per Call Basis)**

callEventNotification
 notificationType
 eventDescription
 correlationId
 callingParticipant
 callingParticipantName
 callingParticipantAlternate
 calledParticipant
 callingParticipantPrivacy
 callSessionIdentifier
 addressDirection:
 originatorTasId:
 callingParticipantAccessNetworkInfo
 callbackData
 link

 action
 actionToPerform
 displayName
 routingAddress
 decisionId
 displayAddress
 callInfo

These are additional Parameters Call Direction Response API (CR 245)

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

CTN (including AT&T/FN/Cricket customers)

Service tier (like Basic vs. Advanced)

Service Tags:

- FirstNet
- CRU
- COU
- Customers who have rate-plan-included Advanced service.
- Cricket
- Prepaid
- Wireless Home Phone

ActiveArmor Application Data

TN from Device Address Book - Hashed (shared only with explicit subscriber consent)

Device OS

ActiveArmor Version Information

The value generated based at least in part on information associated with the calling device may be generated from Defendants, a third party (e.g., Hiya), or some combination thereof.

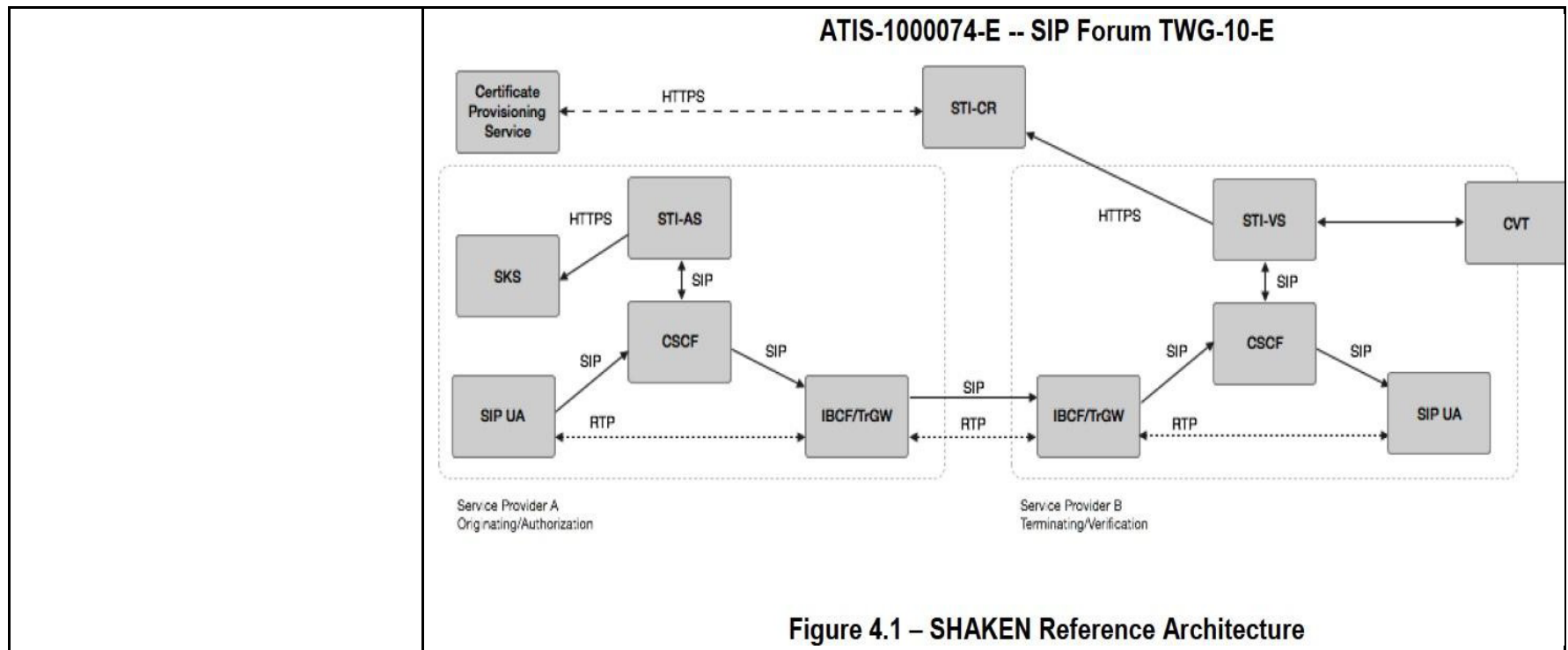
For example, Enterprise Caller Scoring is a score generated for the calling device that indicates the validity of a phone number. *See, e.g., Enterprise Caller Scoring - Stop spammers no matter what phone numbers they use*, Hiya Protect, RQ-ATT0000286-RQ-ATT0000291 (<https://www.hiya.com/products/enterprise-caller-scoring>):

How it Works

Enterprise Caller Scoring is a new layer of Hiya's Adaptive AI that stops number rotation — the practice of switching phone numbers to avoid spam detection — from being effective on mobile networks.

Like a credit agency for enterprise callers, Enterprise Caller Scoring assesses incoming calls based on the calling enterprise's history across all the numbers they own. It can identify the calling enterprise's reputation for more than 150 million enterprise phone numbers in the US — even phone numbers that haven't yet built a calling history. An enterprise's reputation continuously evolves based on behavior and is automatically recognized across all their numbers.

	<i>See also</i> Michelle Wallace, <i>How Hiya’s Proprietary Adaptive AI Stops Phone Spam</i>, Hiya Protect, https://blog.hiya.com/how-hiyas-proprietary-adaptive-ai-stops-phone-spam. Both the value and the score generated for the calling device may be generated by Defendants’ systems, a third party (e.g. Hiya) at Defendant’s request or direction, or some combination thereof. The value and score can be used to detect spoofed, spam and/or fraudulent phone calls. As another example, the Accused Instrumentalities use a verification service that receives information pertaining to a call initiated by a calling device. <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/). As another example, Call Protect, ActiveArmor, and/or the ActiveArmor mobile application use a verification service within Defendants, a third party (e.g., Hiya), or a combination thereof. As another example, STIR/SHAKEN technology comprises a verification service provider (STI-VS). <i>See, e.g.</i>, RQ0001970 (https://stiga.atis.org/resources/):
--	--



This SHAKEN reference architecture includes the following elements:

- SIP UA – The SIP User Agent authenticated by the service provider network. When the SIP UA is under direct management control of the telephone service provider, the service provider network can assert the calling party identity in originating SIP INVITE requests initiated by the SIP UA.
- IMS/Call Session Control Function (CSCF) – This component represents the SIP registrar and routing function. It also has a SIP application server interface.
- Interconnection Border Control Function (IBCF)/Transition Gateway (TrGW) – This function is at the edge of the service provider network and represents the Network-to-Network Interface (NNI) or peering interconnection point between telephone service providers. It is the ingress and egress point for SIP calls between providers.
- Authentication Service (STI-AS) – The SIP application server that performs the function of the authentication service defined in ~~draft-ietf-stir-rtc4474bis~~[RFC 8224](#). It should either itself be highly secured and contain the Secure Key Store (SKS) of secret private key(s) or have an authenticated, Transport Layer Security (TLS)-encrypted interface to the SKS that stores the secret private key(s) used to create PASSporT signatures.
- Verification Service (STI-VS) – The SIP application server that performs the function of the verification service defined in ~~draft-ietf-stir-rtc4474bis~~[RFC 8224](#). It has an Hypertext Transfer Protocol Secure (HTTPS) interface to the Secure Telephone Identity Certificate Repository that is referenced in the Identity header field to retrieve the provider public key certificate.
- Call Validation Treatment (CVT) – This is a logical function that could be an application server function or a third party application for applying anti-spoofing mitigation techniques once the signature is positively or negatively verified. The CVT can also provide information in its response that indicates how the results of the verification should be displayed to the called user.
- SKS – The Secure Key Store is a logical highly secure element that stores secret private key(s) for the authentication service (STI-AS) to access.
- Certificate Provisioning Service – A logical service used to provision certificate(s) used for STI.
- Secure Telephone Identity Certificate Repository (STI-CR) – This represents the publically accessible store for public key certificates. This should be an HTTPS web service that can be validated back to the owner of the public key certificate.

As one example, the SIP Identity header is generated from information associated with the device. *See, e.g.*, RQ0001970 (<https://sti-ga.atis.org/resources/>). As one example, the SIP Identity header comprises the Personal Assertion Token (PASSporT), which is a value generated based at least in part on information associated with the calling device. *See, e.g.*, RQ0001970 (<https://sti-ga.atis.org/resources/>). As one example, the SIP Identity header comprises the Personal Assertion Token (PASSporT), which is a value generated based at least in part on information associated with

the calling device. *See, e.g.*, RQ0001970 (<https://sti-ga.atis.org/resources/>).

4.1 STIR Overview

The documents ~~ietf-stir-rfc4474bis~~[RFC 8224](#) and ~~ietf-stir-passport~~[RFC 8225](#) define a set of protocol level tools that can be used in Session Initiation Protocol (SIP) for applying digital signatures to the Caller ID or telephone number of the calling party.

4.1.1 Personal Assertion Token (PASSporT) ~~Token~~

The document ~~ietf-stir-passport~~[RFC 8225](#) defines a token-based signature that combines the use of JavaScript Object Notation (JSON) Web Tokens, JSON Web Signatures, and X.509 certificate key pairs, or Public Key Infrastructure (PKI), to create a trusted signature. The authorized owner of the certificate used to generate the signature can be validated and traced back to the known trust anchor who signed the certificate. The Personal Assertion Token (PASSporT) ~~token~~ includes a number of claims the signer of the token is asserting. The associated public certificate is used to verify the digital signature and the claims included in the PASSporT~~token~~. The public certificate is also used to validate the entity that signed the token through a Service Provider Identifier (SPID), as defined in ~~ietf-stir-certificates~~[RFC 8226](#). The validated claims and the validated identity of the entity signing the claims can both be used to determine the level of trust in the originating entity and their asserted calling party information. Call blocking applications or other mitigation techniques could use the information over time to determine “reputation” of the entity signing the token, which could provide further input to determine the level of trust for the calling party information. Note that PASSporT~~s~~~~tokens~~ and signatures themselves are agnostic to network signaling protocols but are used in ~~draft-ietf-stir-rfc4474bis~~[RFC 8224](#) to define specific SIP usage as described in the next section.

See also J. Peterson et al., *Authenticated Identity Management in the Session Initiation Protocol (SIP)*, Internet Engineering Task Force (Feb. 2018), RQ0001971-RQ0002016 (<https://tools.ietf.org/html/rfc8224>).

Step 4: Populate and Add the Identity Header

Subsequently, the authentication service **MUST** form a PASSport object and add a corresponding Identity header field to the request containing either the full or compact form of PASSport. For the baseline PASSport header (headers containing no "ppt" parameter), this follows the procedures in [Section 4](#); if the authentication service is using an alternative "ppt" format, it **MUST** add an appropriate "ppt" parameter and follow the procedures associated with that extension (see [Section 9](#)). After the Identity header field has been added to the request, the authentication service **MUST** also add an "info" parameter to the Identity header field. The "info" parameter contains a URI from which the authentication service's credential can be acquired; see [Section 7.3](#) for more on credential acquisition.

6.2. Verifier Behavior

This document specifies a logical role for SIP entities; this role is called a verification service, or verifier. When a verifier receives a SIP message containing one or more Identity header fields, it inspects the signature(s) to verify the identity of the originator of the message. The results of a verification are provided as input to an authorization process that is outside the scope of this document.

See also C. Wendt & J. Peterson, *PASSport: Personal Assertion Token*, Internet Engineering Task Force (Feb. 2018), RQ0002017-RQ0002041 (<https://datatracker.ietf.org/doc/html/rfc8225>).

	PASSportT specifically uses this token format and defines claims that convey the identity of the origination and destination of personal communications. The primary value asserted in a PASSportT object is the originating identity representing the identity of the calling party or the initiator of a personal-communications session. The signer of a PASSportT object may or may not correspond to the originating identity. For a given application's use or using protocol of PASSportT, the creation of the PASSportT object is performed by an entity that is authoritative to assert the caller's identity. This authority is represented by the certificate credentials and the signature, and the PASSportT object is created and initiated to the destination(s) per the application's choice of authoritative point(s) in the network. For example, the PASSportT object could be created at a device that has authenticated with a user or at a network entity with an authenticated trust relationship with that device and its user. Destination identities represent the intended destination of the personal communications, i.e., the identity(s) being called by the caller. The destination point or points determined by the application need to have the capability to verify the PASSportT and the digital signature. The PASSportT-associated certificate is used to validate the authority of the originating signer, generally via a certificate chain to the trust anchor for that application.
--	---

Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP)

Alliance for Telecommunications Industry Solutions

Approved October 2015

Abstract

This specification defines best practices for obtaining the device identifiers (e.g., International Mobile Equipment Identity [IMEI]) from mobile devices even if the mobile device is locked or disabled. This best practices specification was developed in response to Recommendation 1.5 of the December 4, 2014 Federal Communications Commission (FCC) Technological Advisory Council (TAC) report on Mobile Device Theft Prevention (MDTP).

5.2.4 Origination Identifier (“origid”)

In addition to attestation, the unique origination identifier (“origid”) is defined as part of SHAKEN. This unique origination identifier should be a globally unique string corresponding to a Universally Unique Identifier (UUID) (RFC 4122).

The purpose of the unique origination identifier is to assign an opaque identifier corresponding to all or part of the originating service provider’s network (data centers, IBCF nodes, access networks, IMS core complexes, etc.) ~~initiated calls themselves~~, customers, customer or interconnecting service provider nodes, classes of customer devices, or other groupings that a service provider might want to use to indicate common call sources for determining things such as reputation or trace back identification of customers or gateways.

The origid is not intended to directly expose or be reverse-engineered to a customer or service provider identity, but it should be useful for analytics purposes in remote networks and traceback within the originating service provider network.

Best practices will specify when it is appropriate to use groupings less-granular than per-customer, customer device or node, or interconnecting service provider or interconnecting service provider node for origination identifier marking. Where origination identifier granularity is at the customer level or finer, best practices should also cover methods to protect the privacy of individual customers whose identity might be deduced through calling patterns. ~~For Full Attestation, in general, a single identifier will be used as part of the certificate representing direct service provider initiated calls on its VoIP network. A service provider may, for example, also choose to have a pool of identifiers to differentiate geographic regions or classes of customers. Best practices will likely develop as trace back and illegitimate call identification practices evolve.~~

~~For Partial Attestation, a single identifier per customer is required in order to differentiate calls both for trace back and reputation segmentation so that one customer’s reputation doesn’t affect other customer’s or the service provider’s call reputation. A service provider may choose to be more granular (e.g., per node per customer) depending on its size and classes of services that the service provider offers.~~

~~For Gateway Attestation, best practices will dictate that the “origid” should be sufficiently granular to identify the originating node or trunk to allow for trace back identification and reputation scoring.~~

AT&T further discloses that the Accused Instrumentalities receive and use the following information associated with the calling device. *See, e.g.,* RQ-ATT0000070-RQ-ATT0000086 (<https://about.att.com/privacy/privacy-notice.html>):

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

	The information we collect x To better run our business, we collect information about you, your equipment and how you use our products and services. This can include: • Account information. You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including Customer Proprietary Network Information. • Equipment information. We collect information about equipment on our network like the type of device you use, device ID, and phone number. • Network performance. We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working. • Location information. Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites. • Web browsing and app information. We automatically collect a variety of information which may include time spent on websites or apps, website and IP addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information. • Biometric information. Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our Biometric Information Privacy Notice. • Third-party information. We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T.
--	--

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

	How we use your information × We rely on the information we collect to support our business functions, power our services and improve your experience, such as when we: • Combine it with the information from testing and running our network to determine which products and services better meet the needs of our customers. • Provide our products and services. • Contact you. • Improve your experience and safety. This includes verifying your identity, detecting and preventing fraud, protecting your financial accounts, authorizing transactions and assisting your interactions with customer care. • Improve and protect our network. • Use it to help understand which additional products and services may interest you and others. (We don’t access or use the content of your texts, emails or calls for this or any other marketing and advertising.) • Design and deliver advertising, marketing and promotional campaigns to you and others – and measuring their effectiveness (See your choices). • Use it for billing, collection, and protection of our property and legal rights. • Prevent and investigate security issues, illegal activities, and violations of our terms and conditions. • Conduct research and create aggregated reports – reports that offer insights about groups of customers, but not individuals (we do not attempt to re-identify individuals in aggregated reports). <i>See also AT&T ActiveArmor Mobile Security Application and Service, AT&T, RQ-ATT0000139-RQ-ATT0000150 (https://www.att.com/legal/terms.activeArmorMobileSecurity.html):</i>
--	--

In order to perform the functions of the Service including but not limited to its Call Features, AT&T may use and/or disclose or allow the disclosure to our third-party vendor(s) of Your personal information, including without limitation mobile number, contacts/address book in order to populate detail in the call detail screen, the presence or absence of calling party phone numbers in your Device address book, and App usage information, such as which numbers you report and/or manually block within the App, as factors to determine which callers are suspected fraud and spam. The contact names and phone numbers in your Device address book are not shared for any purpose other than improving your experience with the App by helping you to recognize known callers.

3.2 Consent for Information Disclosure in Connection with Data Features

The Service includes the following data security and related features: **Device Security Alerts, Data Breach Alerts, Public Wi-Fi Protection (VPN & Wi-Fi Alerts), Identity Monitoring, Reverse Number Lookup, Safe Browsing, and Device Theft Alerts** (collectively “Data Features”)

In order to perform the functions and to improve the effectiveness of the Service including but not limited to its Data Features for all users, AT&T, its pertinent suppliers and their subsidiaries, agents and subcontractors may collect, maintain, process, use, and disclose diagnostic, technical, usage and related information including, but not limited to, information about:

- the type of Device You are using and the operating system You are running;
- Your applicable wireless network provider/carrier;
- the applications and files present on Your Device and SD memory card;
- the results of any scans performed by the App; and
- actions You take as a result of any virus or malware notifications.

We also may collect information about how the App and any associated Service applications behave on Your Device and the network services with which applications installed on Your Device communicate in order to determine if any applications are behaving maliciously (for example, is an application accessing Your address contacts, sending premium-rate text messages that charge money to Your wireless bill, or communicating with a server known to host phishing websites).

As one example, within the Accused Instrumentalities, the received information pertaining to the call includes a score generated for the calling device, the score indicating a validity of a phone number. For example, the score generated for the calling device comprises and/or has as an input or signal, among other inputs and/or signals, an indication of the attestation level associated with the calling device and indicates a validity of a phone number, but the score is not limited to the A or B or C attestation level. *See, e.g.*, RQ0001970 (<https://sti-ga.atis.org/resources/>).

5.2.3 Attestation Indicator (“attest”)

The “attest” claim allows the originating service provider that is populating an Identity header to clearly indicate the information it can vouch for regarding the origination of the call.

~~This indicator allows for both identifying the service provider that is vouching for the call as well as clearly indicating what information the service provider is attesting to.~~

In the SHAKEN framework we define the following three levels of attestation:

A. Full Attestation: The signing provider shall satisfy all of the following conditions:

- Is responsible for the origination of the call onto the IP-based service provider voice network.
- Has a direct authenticated relationship with the customer and can identify the customer.
- Has established a verified association with the telephone number used for the call.

NOTE 1: The signing provider is asserting that their customer can “legitimately” use the number that appears as the calling party (i.e., the Caller ID). The legitimacy of the telephone number(s) the originator of the call can use is subject to signer-specific policy, but could use mechanisms such as the following:

- The number was assigned to this customer by the signing service provider.
- This number is one of a range of numbers assigned to an enterprise or wholesale customer.
- The signing service provider has ascertained that the customer is authorized to use a number (e.g., by business agreement or evidence the customer has access to use the number). This includes numbers assigned by another service provider.
- The number is not permanently assigned to an individual customer but the signing provider can track the use of the number by a customer for certain calls or during a certain timeframe.

NOTE 2: Ultimately it is up to service provider policy to decide what constitutes “legitimate right to assert a telephone number” but the service provider’s reputation may be directly dependent on how rigorous they have been in making this assertion.

B. Partial Attestation: The signing provider shall satisfy all of the following conditions:

- Is responsible for the origination of the call onto ~~its-the~~ IP-based service provider voice network.
- Has a direct authenticated relationship with the customer and can identify the customer.
- Has NOT established a verified association with the telephone number being used for the call.

9

ATIS-1000074-E -- SIP Forum TWG-10-E

NOTE: By populating this value, the service provider attests that it can trace the source of the call to a customer for policy enforcement purposes. ~~When partial attestation is used, each customer will have a unique origination identifier created and managed by the service provider, but the intention is that it will not be possible to reverse engineer the identity of the customer purely from the identifier or signature. As described in section 5.2.4, the unique origination identifier allows data analytics to establish a reputation profile and assess the reliability of information asserted by the customer assigned this unique identifier. The identifier also provides a reliable mechanism to determine the customer for forensic analysis or legal action where appropriate.~~

~~The verifier validates that the PASSporT token provided in the Identity header of the INVITE includes all of the baseline claims, as well as the SHAKEN extension claims. The verifier shall also follow the draft-ietf-stir-#64474bis~~ RFC 8224-defined verification procedures to check the corresponding date, originating identity (i.e., the originating telephone number) and destination identities (i.e., the terminating telephone numbers), with the restrictions specified in this section.

	C. Gateway Attestation: The signing provider shall satisfy all of the following conditions: ~~Is the entry point of the call into its VoIP network.~~ - Has no relationship with the initiator of the call (e.g., international gateways). ~~NOTE: The token will provide a unique origination identifier of the node in the “origid” claim. (The signer is not asserting anything other than “this is the point where the call entered my network”.)~~ <u>NOTE: The signer/originating service provider should be able to trace a call to an interconnecting service provider and/or peer node for traceback or policy enforcement purposes. Gateway attestation may also be used when the STI-AS does not have sufficient information for determining that A or B attestation applies even when the call was received at a customer interface.</u> For the PASSporT extension claim, the “attest” key value pair shall be set to uppercase characters “A”, “B”, or “C” corresponding to the appropriate attestation defined above. An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
27[b] performing a security determination based at least in part on the score generated for the calling device, and at least in part by verifying the value included in the information pertaining to the call initiated by the call-ing device; and	The Accused Instrumentalities perform a security determination based at least in part on the score generated for the calling device, and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device. The Accused Instrumentalities perform and/or are capable of performing a security determination based at least in part on the score generated for the calling device and at least in part by verifying the value included in the information pertaining to the call, from Defendants, a third party (e.g. Hiya), or some combination thereof. <i>See e.g.,</i> https://work.hiya.com/adaptive-ai-ebook

Adaptive AI: A Proactive Strategy for Stopping Scam and Fraud Calls

Adaptive AI is an innovative new feature of Hiya Protect, a proprietary call protection service used by carriers, distribution partners and the Hiya mobile app.

Unlike other capabilities on the market today, Adaptive AI uses machine learning to proactively hunt and shut down scam campaigns. With the ability to stay ahead of scammers, Adaptive AI works in real-time, without the need for human intervention or any updating of existing AI models.

For example, the value generated based at least in part on information associated with the calling device can include a device fingerprint, device information (e.g., make, model, serial number, operating system version, application information, or other identifying information of a device), customer account information, location information, caller or callee number, or other information associated with the device and upon which (or upon verification of which) a security determination is in part based. The value generated based at least in part on information associated with the calling device may be generated from Defendants, a third party (e.g., Hiya), or some combination thereof and is verified as part of the security determination when deciding to connect, convey assurance of the callee, convey a failure to confirm the callee, and/or refuse to connect the initiated call.

For example, Defendant’s Robocall mitigation system performs a security determination based at least in part on the score generated for the calling device, and at least in part by verifying the value. *See* ATT-RQ_0000042, -43, -44 (evidencing device specific data, device settings, installed applications e.g., ActiveArmor, system or application software versions (e.g., “Device OS”, “ActiveArmor Version Information”), contact list data (TN from Device Address Book), or other data associated with the calling device is stored and shared with AT&T’s “Vendor/Partner Hiya”). These values are used, along with one or more scores to determine the validity of a phone number. Furthermore, the score and value are used in the process of conveying assurance or failure to confirm for intra- and inter- network calls.

Active Armor Data Elements

As part of the Active Armor Robocall mitigation program, data elements related to calling are shared with our Vendor/Partner Hiya. Note that Hiya’s usage and management of these data elements is under written agreement with AT&T.

AT&T GFMO (Global Fraud Management Office) and AT&T CDO (Chief Data Office) each provide a set of per-Number data elements. AT&T CTS/PRS uses an API to provide per-Call data elements. There are additional data elements that are under investigation to determine if they will have value in Robocall Mitigation.

The following is a listing of each data element, by data source. See attached spreadsheet for more details.

AT&T CTS/PRS**Call Direction Response API (Per Call Basis)**

callEventNotification
 notificationType
 eventDescription
 correlationId
 callingParticipant
 callingParticipantName
 callingParticipantAlternate
 calledParticipant
 callingParticipantPrivacy
 callSessionIdentifier
 addressDirection:
 originatorTasId:
 callingParticipantAccessNetworkInfo
 callbackData
 link

 action
 actionToPerform
 displayName
 routingAddress
 decisionId
 displayAddress
 callInfo

These are additional Parameters Call Direction Response API (CR 245)

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

CTN (including AT&T/FN/Cricket customers)

Service tier (like Basic vs. Advanced)

Service Tags:

- FirstNet
- CRU
- COU
- Customers who have rate-plan-included Advanced service.
- Cricket
- Prepaid
- Wireless Home Phone

ActiveArmor Application Data

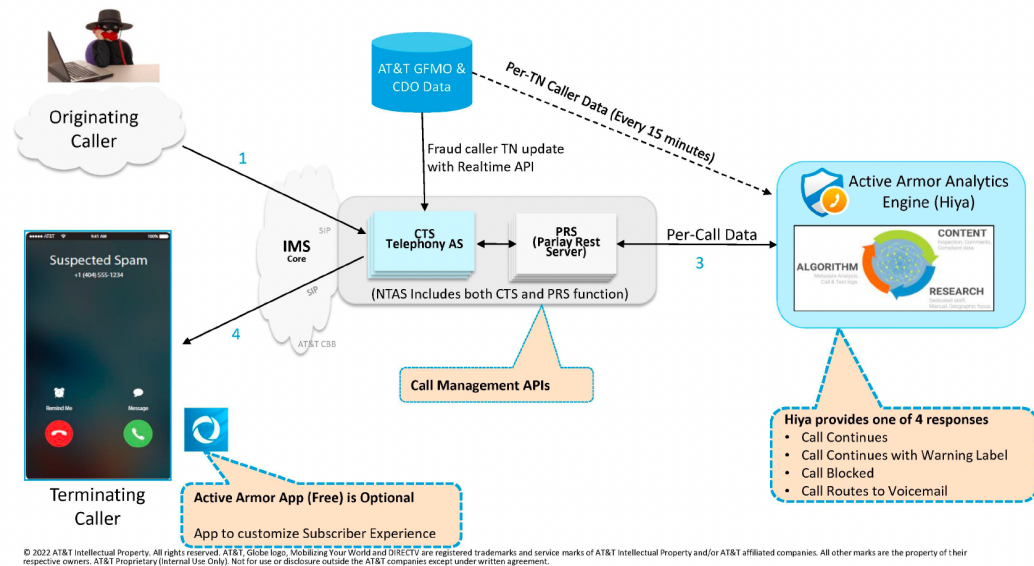
TN from Device Address Book - Hashed (shared only with explicit subscriber consent)

Device OS

ActiveArmor Version Information

See, e.g., ATT-RQ_0000045 showing that Hiya provides at least one of 4 responses – namely, “Call Continues,” “Call Continues with Warning Label”, “Call Blocked” or “Call Routes to Voicemail” (e.g., whether or not the call should be connected or blocked).

AT&T Active Armor (Call Protect) – High Level Architecture



RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

ATT-RQ_0000045

As another example, Enterprise Caller Scoring is a score generated for the calling device that indicates the validity of a phone number. *See, e.g., Enterprise Caller Scoring - Stop spammers no matter what phone numbers they use, Hiya Protect, RQ-ATT0000286-RQ-ATT0000291* (<https://www.hiya.com/products/enterprise-caller-scoring>):

How it Works

Enterprise Caller Scoring is a new layer of Hiya's Adaptive AI that stops number rotation — the practice of switching phone numbers to avoid spam detection — from being effective on mobile networks.

Like a credit agency for enterprise callers, Enterprise Caller Scoring assesses incoming calls based on the calling enterprise's history across all the numbers they own. It can identify the calling enterprise's reputation for more than 150 million enterprise phone numbers in the US — even phone numbers that haven't yet built a calling history. An enterprise's reputation continuously evolves based on behavior and is automatically recognized across all their numbers.

See also <https://blog.hiya.com/how-hiyas-proprietary-adaptive-ai-stops-phone-spam>.

As another example, the Accused Instrumentalities perform a security determination based at least in part on the SIP Identity header. The SIP Identity header is based at least in part on the score

	generated for the calling device, and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device. <i>See, e.g.,</i> RQ0001970 (https://sti-ga.atis.org/resources/). As one example, the Accused Instrumentalities perform a security determination based at least in part on a public certificate, which is verifying the value comprised in the SIP Identity header included in the information pertaining to the call initiated by the calling device. As one example, the value is the Personal Assertion Token (PASSporT). [The verifier validates that the PASSporT ~~token~~ provided in the Identity header of the INVITE includes all of the baseline claims, as well as the SHAKEN extension claims. The verifier shall also follow the ~~draft-ietf-stir-#fc4474bis~~RFC 8224-defined verification procedures to check the corresponding date, originating identity (i.e., the originating telephone number) and destination identities (i.e., the terminating telephone numbers), <u>with the restrictions specified in this section</u>. As one example, the Accused Instrumentalities perform a security determination based at least in part on the attestation level. The attestation level is based at least in part on the score generated for the calling device and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device. <i>See, e.g.,</i> RQ0001970 (https://sti-ga.atis.org/resources/).
--	--

Use of standardized cryptographic digital signatures to validate the originator of a signed identity can provide a verifiable mechanism to identify the authorized originator of a call into the VoIP network with non-repudiation. Further, the use of an assigned attestation indicator and a unique origination identifier depending on how and where the call is originated in the VoIP network represents the originating signer’s ability to vouch for the accuracy of the source of origin of the call. For example, if the service provider has an authenticated direct relationship with the origination of the call, this attestation is categorized differently than calls that are originated from different networks or gateways that the service provider may have received from an unauthenticated network or that are

3

ATIS-1000074-E -- SIP Forum TWG-10-E

unsigned. Verifiers of signatures will use these attestations as information to provide trace back mechanisms, as well as information to feed into any call spam identification solution enabled on behalf of their customer.

5.2.2 PASSporT Extension “shaken”

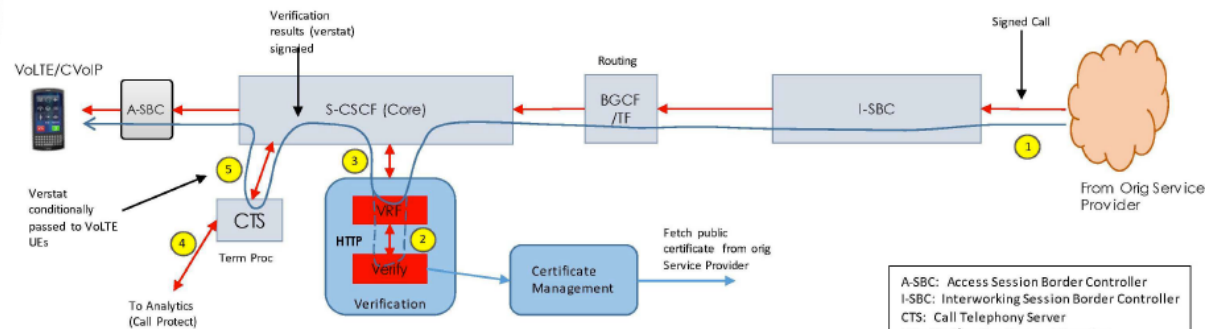
The base PASSporT set of claims cover the assertion of the originating telephone number along with date and destination telephone numbers to avoid replay attacks using valid Identity header fields. draft-ietf-stir-passport-shaken defines ~~This section will detail a specific the “shaken” extension to the PASSporT to cover the following requirements of SHAKEN. The SHAKEN “shaken” extension to PASSporT shall be implemented with all extension claims as part of the signed PASSporT token.~~

1. The ability to provide an attestation indicator for the context of how the call was originated.
2. The ability to provide a unique originating identifier, as described in Section 5.2.4, that can serve as an opaque indication of where in the originating service provider’s network the call was originated. ~~This identifier shall be globally unique and consistent so it can be used in analytics for tracking the reputation of a particular originating service and could also be used for any traceback efforts if a particular originator is a consistent or pervasive “bad actor”.~~

The PASSporT “shaken” extension shall include both an attestation indicator (“attest”), as described in section 5.2.3 and an origination identifier (“origid”) as described in section 5.2.4. The SHAKEN PASSporT ~~token~~ would have the form given in the example below:

As another example, intra-network calls may be treated differently from inter-network calls. The attestation level of a call may be included within a verstat (verification indicator) tag, or other header. *See e.g., ATT-RQ-466, 467.*

Inter-Network SHAKEN Flows (ATT terminated)



1. Signed call is received from an originating carrier that supports SHAKEN. Terminating S-CSCF detects the received Identity header and sends the call to the VRF.
2. The VRF formulates the HTTP verification request and sends the request to the Verification Server.
3. The verification results are returned and signaled in the "verstat" parameter (contained in PAI/From headers).
4. Verstat is used by analytics (e.g., Call Protect) as an input to reputation scoring.
5. Verstat is conditionally passed to terminating VoLTE UE and UE uses this information to influence the calling number/name display information. For CVoIP, term CTS modifies the Calling Number to include SHAKEN verification results.

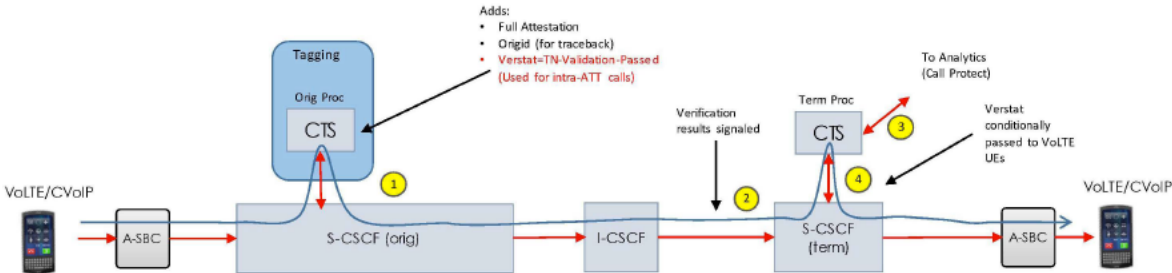
AT&T Proprietary and Confidential

This document and information contained therein is not for use or disclosure outside of AT&T

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

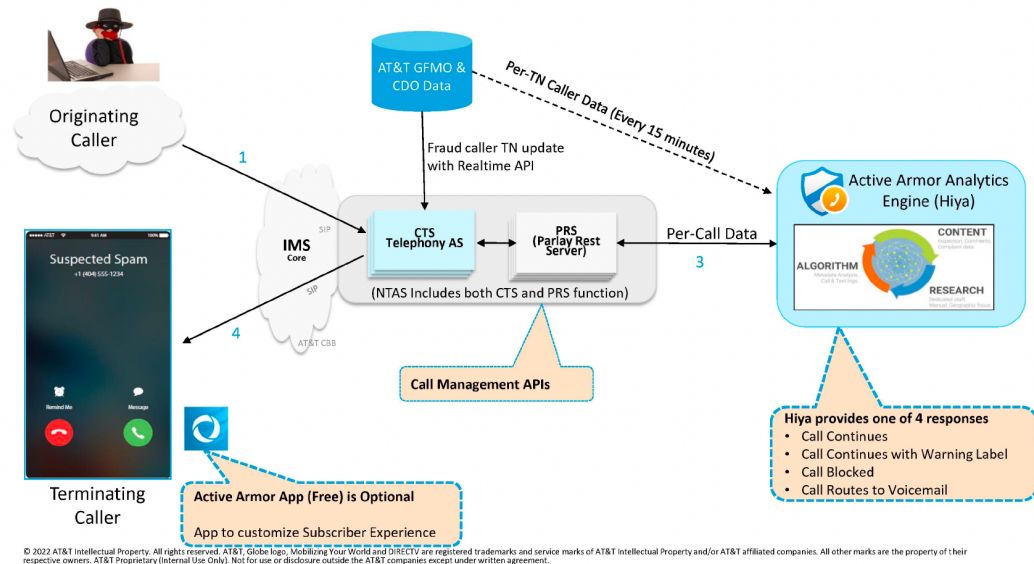


ATT-RQ_0000466

	Intra-AT&T SHAKEN Flows  - After originating processing is completed, CVoIP/VoLTE calls will be “tagged”. - Tagging adds verstat parameter to emulate a call that was verified successfully. This is used for intra-network (ATT to ATT) calls. - Intra-ATT calls are not “signed” - The emulated verification result (verstat) is passed to CTS. - Verstat is used by analytics (e.g. Call Protect) as an input to reputation scoring. - Verstat is conditionally passed to terminating VoLTE UE and UE uses this information to influence the calling number/name display information. For CVoIP, term CTS modifies the Calling Number to include SHAKEN verification results. A-SBC: Access Session Border Controller CTS: Call Telephony Server I-CSCF: Interrogating Call Session Control Function S-CSCF: Serving Call Session Control Function AT&T Proprietary and Confidential This document and information contained therein is not for use or disclosure outside of AT&T ATT-RQ_0000467
27[c] based at least in part on the security determination, performing at least one of conveying an assurance to a callee associated with the call or conveying a failure to confirm to the callee associated with the call.	The Accused Instrumentalities, based at least in part on the security determination, perform at least one of conveying an assurance to a callee associated with the call or conveying a failure to confirm to the callee associated with the call. <i>See, e.g.,</i> ATT-RQ_0000045 (Hiya provides at least one of four responses – namely, “Call Continues,” “Call Continues with Warning Label”, “Call Blocked” or “Call Routes to Voicemail”

(e.g., whether or not the call has an assurance or a failure of an assurance)):

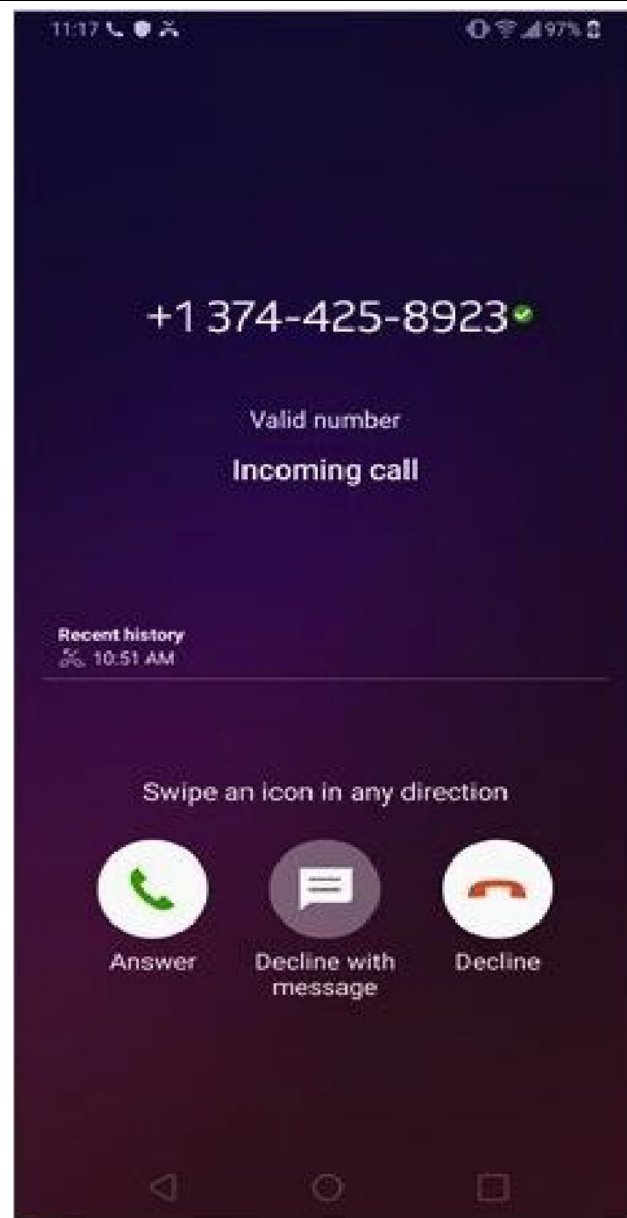
AT&T Active Armor (Call Protect) – High Level Architecture



RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

ATT-RQ_0000045

As one example, based at least in part on the security determination, the Accused Instrumentalities convey an assurance to a callee associated with the call, including but not limited to conveying a green check, “valid number,” or “[V]”, brand logos, contact/caller name, and/or otherwise providing call logs, reports, or other indications reflecting confirmation. *See, e.g.,* RQ-ATT0000024-RQ-ATT0000026 (https://about.att.com/story/2019/call_validation_displays.html):



*Samsung Galaxy S10, Galaxy S10+, LG V40 ThinQ and AT&T Digital Home
Phone Service Can Now Show That a Call Is Authenticated*

AT&T* has turned on its first phone displays that let you know an incoming call is really from the number appearing on Caller ID. This fights against “spoofing” of phone numbers – a trick used by many illegal robocallers.

Most AT&T customers with a Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ™ will see a special display when an incoming call has been authenticated. They will see a green checkmark and the words, “Valid Number.”

Consumers with AT&T Phone digital home phone service also can activate the feature. It will give them a “[V]” for valid number.

Phone service providers have jointly developed a technology – the SHAKEN/STIR standards – to digitally validate calls. This won’t solve the problem of unwanted robocalls by itself. But it can give consumers greater confidence and control over the calls they answer.

“This is another step to tame annoying, unwanted robocalls,” said Kevin Petersen, AT&T senior vice president, Postpaid Wireless Products. “In the coming year, we’ll continue to take more steps and put more pressure on the bad guys.”

AT&T is rolling out its SHAKEN/STIR display as part of its AT&T Call Protect service, which is being added at no charge to millions of mobility consumer lines. AT&T Call Protect blocks or labels suspected illegal and unwanted robocalls.

This strategy will give a multiplier effect to call protection: A “valid number” on an AT&T device means the incoming call has been authenticated by SHAKEN/STIR *and* passed through AT&T Call Protect screening.

Here are some other key points:

- A call that shows “valid number” has been verified and can increase your trust level. But a call without the label may still be a legitimate call. More calls will be marked with “valid number” over time, as more network providers implement SHAKEN/STIR and link to each other.
- AT&T has rolled out AT&T Call Protect automatically to many Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ users. Others are on the way soon.¹ If you’re not seeing call validation on those devices when you accept their latest software update, you don’t have to wait. You can download the AT&T Call Protect app, or turn on the service from your account settings in myAT&T.
- AT&T Phone digital home phone users can opt-in to get AT&T Digital Phone Call Protect and call validation. Just go to your account settings on myAT&T and turn it on.
- Validation displays will be added to more mobile devices in the new year.
- Finally, a “valid number” display helps fight against bad guys, but it can never guarantee an individual caller is a good guy. Consumers should always use their best judgement when answering calls from strangers.

See, e.g., RQ-ATT0000137-RQ-ATT0000138 (<https://www.att.com/support/article/u-verse-voice/KM1235421/>):

Digital Phone Call Protect features

Here's what you get with Digital Phone Call Protect¹:

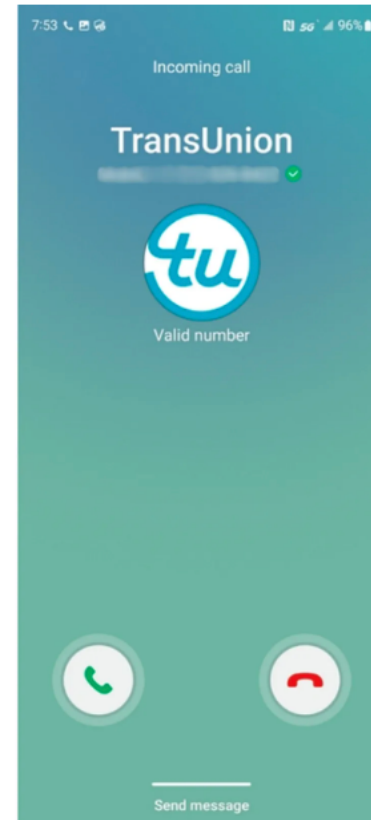
- **Call validation:** Soon you'll see a [V] on your caller ID for some calls. This means we've confirmed that the call originated from the phone registered to that number. (Remember to still be cautious when answering a call from an unknown number.)
- **Automatic fraud blocking:** Each potential fraud call gives the caller a busy signal, and the call won't go through. You can toggle this feature on or off.
- **Call blocking:** If you have a specific number you want to block, press *61 after the unwanted call to block that number.
- **Call log:** You can see detailed call log info.
- **Suspected spam call warning:** Your caller ID will show Suspected Spam and a type (Political, Nonprofit, Telemarketer, Survey, or Robocaller).

See also AT&T Will Warn You of Incoming Robocalls – But Not on iPhone, AT&T, RQ-ATT0000088-RQ-ATT0000090 (<https://www.idropnews.com/news/fast-tech/att-will-warn-you-of-incoming-robocalls-but-not-on-iphone/125657/>):

It's worth noting that AT&T also offers call verification for iPhone users, *but it won't show up when the call is coming in.*

- To see if a number is verified on iPhone, you'll need to check your call log in the **Phone app** under **Recents**.
- Verified unknown calls will have a checkmark next to them on recent versions of iOS. This clunky method is likely to change in the future, however.

See, e.g., RQ-ATT0000091-RQ-ATT0000094 (<https://www.cnet.com/tech/mobile/at-t-adopts-new-robocall-fighting-tool-that-adds-logo-images-to-caller-id/>):



An example of a company logo that appears when a carrier uses Branded Call Display to authenticate a call.

As another example, based at least in part on the security determination, the Accused Instrumentalities convey and/or are configured to convey a failure to confirm to the callee associated with the inter- or intra- network call, including but not limited by conveying “Unknown caller,” any indication of a potential spoofed, spam, or fraudulent call, such as “suspected spam” or “suspected fraud,” any indication a call was blocked, and/or by with an allowed communication not conveying an assurance such as a green check, “valid number,” or “[V]”, a brand logo, contact/caller name, or providing a call log, report, or other indication reflecting confirmation.

	<i>See, e.g.,</i> RQ-ATT0000095-RQ-ATT0000098 (https://forums.att.com/conversations/account-features/blocking-unknown-numbers/63b33783c1c54d548b8bbe5b). Hey, rehjaeger! The AT&T ActiveArmor application allows you to flag, send to voicemail, and block nuisance & fraud risk calls. You can also send unknown callers to voicemail. To find these settings, you'll open up the AT&T ActiveArmor app then click on the phone icon named Calls. After, you'll scroll down until you see Network Call Preferences. From there, select the drop down arrow listed near Unknown callers and click send to voicemail. Keep in mind, you can only see these settings while connected to your cellular data. To answer your question you can't personally block all unknown callers but you can automatically forward them to your voicemail. We hope we've answered your question! Please let us know if you have additional inquiries! Jonye, AT&T Community Specialist <i>See, e.g.,</i> RQ-ATT0000046-RQ-ATT0000048 (https://about.att.com/blogs/2023/activearmor-text-blocking.html). • We block all the fraud calls we can find. And we label suspected spam calls so you can choose to answer or not. We do this for every customer on our network – more than a billion blocked or labeled calls a month. <i>See, e.g.,</i> RQ-ATT0000051-RQ-ATT0000053 (https://about.att.com/story/2019/att_tmo_call-authentication.html)
--	--

AT&T* and T-Mobile today began rollout of cross-network call authentication based on SHAKEN/STIR standards – another big step toward protecting consumers from unwanted robocalls.

SHAKEN/STIR technology lets consumers know that an incoming call is really coming from the number listed on the caller ID display – not a spoofed robocall or scammer. While authentication won’t solve the problem of unwanted robocalls by itself, it is a key step toward giving customers greater confidence and control over the calls they answer.

For example, a call that is illegally “spoofed” – or shows a faked number – will fail the SHAKEN/STIR Caller ID verification and will not be marked as verified. By contrast, verification will confirm that a call is really coming from the identified number or entity. More calls will be verified over time as more device providers participate, and as more network providers implement the standards.

The FCC has recommended SHAKEN/STIR standards to digitally validate phone calls. The acronym stands for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR).

For more information on all the ways AT&T is protecting customers, visit https://about.att.com/story/2019/att_call_protect.html and <https://att.com/CyberAware>.

See also RQ0001970 (<https://sti-ga.atis.org/resources/>).

The terminating network conveys the verification result to the called user by including a "verstat" parameter in the From and/or P-Asserted-Identity header fields of the INVITE request sent to the called endpoint device, as defined in [TS 24.229].

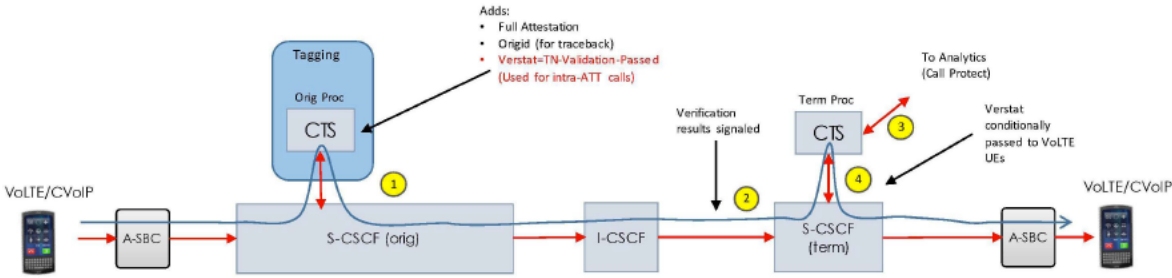
- Call Validation Treatment (CVT) – This is a logical function that could be an application server function or a third party application for applying anti-spoofing mitigation techniques once the signature is positively or negatively verified. The CVT can also provide information in its response that indicates how the results of the verification should be displayed to the called user.

As another example, intra-network calls may be treated differently from inter-network calls. The attestation level of a call may be included within a verstat (verification indicator) tag, or other header. See e.g., ATT-RQ-466, 467.



This document and information contained therein is not for use or disclosure outside of AT&T

ATT-RQ 0000466

	Intra-AT&T SHAKEN Flows  The diagram illustrates the Intra-AT&T SHAKEN Flows. It shows a call path starting from a VoLTE/CVoIP UE, passing through an A-SBC, then an S-CSCF (orig), an I-CSCF, an S-CSCF (term), and finally an A-SBC to another VoLTE/CVoIP UE. Key components include the 'Tagging' block (Orig Proc CTS) and the 'Term Proc CTS'. The flow is numbered 1 through 4, corresponding to the steps listed below. A legend box defines the acronyms: A-SBC: Access Session Border Controller, CTS: Call Telephony Server, I-CSCF: Interrogating Call Session Control Function, S-CSCF: Serving Call Session Control Function. A list of 'Adds' includes Full Attestation, Origid (for traceback), and Verstat=TN Validation-Passed (Used for intra-ATT calls). Arrows indicate the flow of data, including 'Verification results signaled' and 'Verstat conditionally passed to VoLTE UEs'. - After originating processing is completed, CVoIP/VoLTE calls will be "tagged". - Tagging adds verstat parameter to emulate a call that was verified successfully. This is used for intra-network (ATT to ATT) calls. - Intra-ATT calls are not "signed". - The emulated verification result (verstat) is passed to CTS. - Verstat is used by analytics (e.g. Call Protect) as an input to reputation scoring. - Verstat is conditionally passed to terminating VoLTE UE and UE uses this information to influence the calling number/name display information. For CVoIP, term CTS modifies the Calling Number to include SHAKEN verification results. A-SBC: Access Session Border Controller CTS: Call Telephony Server I-CSCF: Interrogating Call Session Control Function S-CSCF: Serving Call Session Control Function AT&T Proprietary and Confidential This document and information contained therein is not for use or disclosure outside of AT&T ATT-RQ_0000467
Claim 28. [pre] A computer program product embodied in a non-transitory computer readable storage medium and comprising computer instructions for:	This is the preamble of the claim and is not limiting. To the extent the preamble is construed as limiting, the Accused Instrumentalities comprise a computer program product(s) embodied in a tangible and non-transitory computer readable storage medium and computer instructions for performing the limitations of the claim. The Accused Instrumentalities, alone and/or in combination, comprise one or more system(s) and service(s) that are configured to perform a security determination and convey an assurance to a callee

	associated with a given call or convey a failure to confirm to the callee, and/or are otherwise capable of detecting, blocking, and preventing SPAM, fraudulent, and spoofed phone calls. <i>See, e.g., Network & Data Security, AT&T, RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security):</i> • Robocall Scam Identification & Mitigation: AT&T has established mechanisms to identify illegal robocall campaigns and help to mitigate them. ◦ Through the complementary programs listed below, AT&T has blocked or labeled billions of unwanted robocalls. ▪ AT&T ActiveArmorSM automatically blocks fraud calls and labels other suspected spam calls so a wireless customer can choose to answer or not. It identifies the calls through data analytics, network intelligence and customer reports. ▪ AT&T’s Global Fraud Management team works closely with the U.S. Telecom Industry Traceback Group and law enforcement to identify the source of illegal calls. This process provides necessary information to stop illegal robocall campaigns and places responsibility on service providers for traffic that originates on their networks. ▪ AT&T’s Global Fraud Management organization, with assistance from the AT&T Chief Data Office, uses sophisticated algorithms to examine billions of calls each day for patterns that indicate a robocalling scheme. They investigate suspicious activity that may be illegal, relying on human fraud expertise before blocking. ◦ Implementation of the caller ID authentication standard known as STIR/SHAKEN remains a top priority for AT&T, and we have deployed it across our IP networks. We have filed comments with the Federal Communications Commission (FCC) detailing our progress on this front and offering our support as the FCC addresses the complex details of implementation. We also supported the TRACED Act, which codified implementation requirements. For example, AT&T advertises “AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature.” <i>See, e.g., RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).</i>
--	---

	How do AT&T and the other major carriers differ in terms of security? ^ AT&T automatically blocks fraud calls in the network before they ring on your phone or fill your voicemail. No action is required to benefit from this security feature. To block your spam calls, you will need to download the free AT&T ActiveArmor mobile security app to set up your network call preferences, customize your robocall protection and create a personal block list. Additionally, you can secure your device and personal data plus receive data breach alerts within the app for no extra cost. ActiveArmor advanced mobile security is \$3.99/month. Advanced security features include Public Wi-Fi Protection, Identity Monitoring, and Reverse Number Lookup. Customers subscribed to AT&T Unlimited ExtraSM and Unlimited PremiumSM get these ActiveArmor advanced security features included with their plan at no extra charge. Details at att.com/unlimited Req's compatible device/service and download of AT&T ActiveArmor Mobile Security app. Data charges may apply. Other terms and req's apply. Details at att.com/activearmorapp. As another example, AT&T advertises that with Digital Phone Call Protect, customers get “call validation,” “Automatic fraud blocking,” and “Suspected spam call warning,” among other features. See, e.g., RQ-ATT0000137-RQ-ATT0000138 (https://www.att.com/support/article/u-verse-voice/KM1235421/):
--	---

Digital Phone Call Protect features

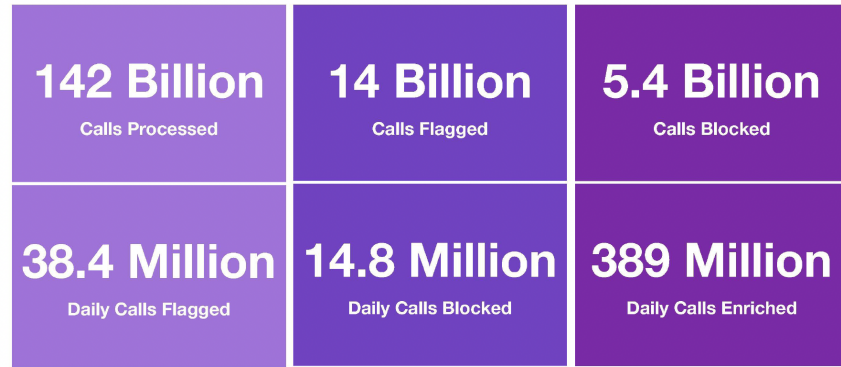
Here's what you get with Digital Phone Call Protect¹:

- **Call validation:** Soon you'll see a [V] on your caller ID for some calls. This means we've confirmed that the call originated from the phone registered to that number. (Remember to still be cautious when answering a call from an unknown number.)
- **Automatic fraud blocking:** Each potential fraud call gives the caller a busy signal, and the call won't go through. You can toggle this feature on or off.
- **Call blocking:** If you have a specific number you want to block, press *61 after the unwanted call to block that number.
- **Call log:** You can see detailed call log info.
- **Suspected spam call warning:** Your caller ID will show Suspected Spam and a type (Political, Nonprofit, Telemarketer, Survey, or Robocaller).

For example, the Accused Instrumentalities comprises one or more processors configured to implement protocols, technologies, features, and services for validating and/or verifying caller identification information including without limitation STIR/SHAKEN.

See, e.g., ATT-RQ_0000001 at 3 (showing volume of blocks calls necessitating the use of computer systems with processors to make the determination to block or connect an outgoing or incoming call):

Hiya-AT&T Call Protect 2023 Summary



3 | HIYA PROPRIETARY AND CONFIDENTIAL

hiya

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

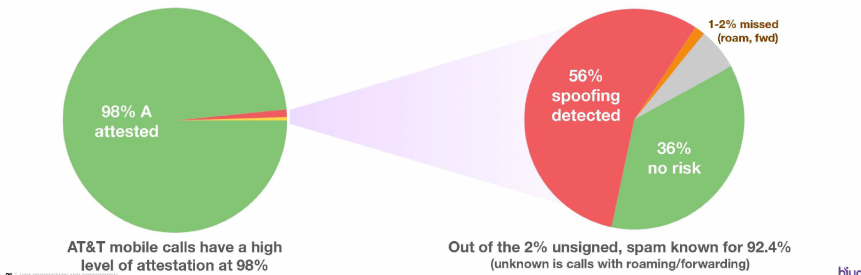
ATT-RQ_0000003

See, e.g., ATT-RQ_0000001 at 26 (showing that AT&T prevents spoofing from its own numbers on its network):

Working with AT&T, Hiya has been successful at preventing spoofing from AT&T phone numbers

STATE OF THE SERVICE TODAY:

Working closely with AT&T, Hiya has solutions in place to address the challenges in mobile spoof detection. Hiya has deployed in production a mobile spoof detection solution that we feel is detecting **98% of spoofed calls using AT&T mobile numbers**, and detecting a large majority of spoofing using other mobile carrier lines.

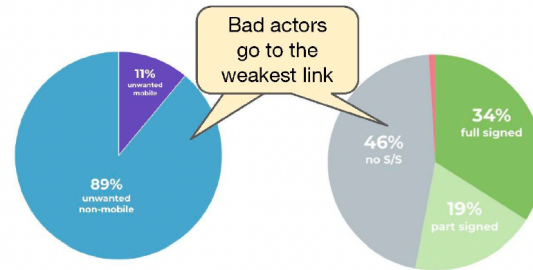


RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

ATT-RQ_0000026

See, e.g., ATT-RQ_0000001 at 28 (noting that call authentication technologies beyond STIR/SHAKEN are required to prevent fraudulent, spam, and spoofed phone calls):

However, the majority of unwanted calls stem from non-mobile sources, and STIR/SHAKEN is far from fixing this issue



89% of unwanted calls are non-mobile originated

with 66% of calls not fully signed

STATE OF THE ECOSYSTEM:

Key impediments on STIR/SHAKEN non-mobile spoofing include:

- Unstable Implementation for Non-Mobile Numbers
- Challenges from Legacy Systems
- Incomplete Adoption Among Service Providers
- Verification and Trust Issues

These complexities provide opportunities for scammers to exploit coverage gaps

Calls from non-mobile sources are much more likely to be unwanted compared to calls from mobile sources

28 | HIYA PROPRIETARY AND CONFIDENTIAL

hiya

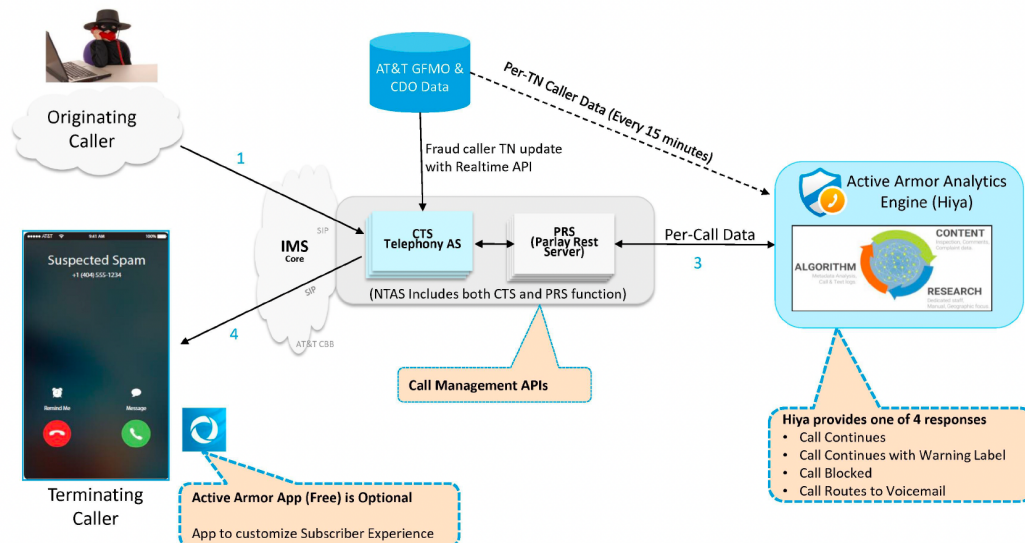
RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

ATT-RQ_0000028

The Accused Instrumentalities are implemented, used, and/or put into service by AT&T in intra- and inter- network communications. See, e.g., RQ-ATT0000051-RQ-ATT0000053 (https://about.att.com/story/2019/att_tmo_call-authentication.html).

	AT&T* and T-Mobile today began rollout of cross-network call authentication based on SHAKEN/STIR standards – another big step toward protecting consumers from unwanted robocalls. SHAKEN/STIR technology lets consumers know that an incoming call is really coming from the number listed on the caller ID display – not a spoofed robocall or scammer. While authentication won’t solve the problem of unwanted robocalls by itself, it is a key step toward giving customers greater confidence and control over the calls they answer. For example, a call that is illegally “spoofed” – or shows a faked number – will fail the SHAKEN/STIR Caller ID verification and will not be marked as verified. By contrast, verification will confirm that a call is really coming from the identified number or entity. More calls will be verified over time as more device providers participate, and as more network providers implement the standards. The FCC has recommended SHAKEN/STIR standards to digitally validate phone calls. The acronym stands for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR). For more information on all the ways AT&T is protecting customers, visit https://about.att.com/story/2019/att_call_protect.html and https://att.com/CyberAware. <i>See, e.g., ATT-RQ_0000045 (Hiya provides at least one of four responses – namely, “Call Continues,” “Call Continues with Warning Label”, “Call Blocked” or “Call Routes to Voicemail” (e.g., whether or not the call has an assurance or a failure of an assurance)):</i>
--	---

AT&T Active Armor (Call Protect) – High Level Architecture



RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

ATT-RQ_0000045

As another example, the Accused Instrumentalities implement STIR/SHAKEN, among other protocols, technologies, features, and services for validating and/or verifying caller identification information. See, e.g., RQ-ATT0000024-RQ-ATT0000026 (https://about.att.com/story/2019/call_validation_displays.html):

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

	AT&T* has turned on its first phone displays that let you know an incoming call is really from the number appearing on Caller ID. This fights against “spoofing” of phone numbers – a trick used by many illegal robocallers. Most AT&T customers with a Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ™ will see a special display when an incoming call has been authenticated. They will see a green checkmark and the words, “Valid Number.” Consumers with AT&T Phone digital home phone service also can activate the feature. It will give them a “[V]” for valid number. Phone service providers have jointly developed a technology – the SHAKEN/STIR standards – to digitally validate calls. This won’t solve the problem of unwanted robocalls by itself. But it can give consumers greater confidence and control over the calls they answer. “This is another step to tame annoying, unwanted robocalls,” said Kevin Petersen, AT&T senior vice president, Postpaid Wireless Products. “In the coming year, we’ll continue to take more steps and put more pressure on the bad guys.” AT&T is rolling out its SHAKEN/STIR display as part of its AT&T Call Protect service, which is being added at no charge to millions of mobility consumer lines. AT&T Call Protect blocks or labels suspected illegal and unwanted robocalls. This strategy will give a multiplier effect to call protection: A “valid number” on an AT&T device means the incoming call has been authenticated by SHAKEN/STIR <i>and</i> passed through AT&T Call Protect screening.
--	---

Here are some other key points:

- A call that shows “valid number” has been verified and can increase your trust level. But a call without the label may still be a legitimate call. More calls will be marked with “valid number” over time, as more network providers implement SHAKEN/STIR and link to each other.
- AT&T has rolled out AT&T Call Protect automatically to many Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ users. Others are on the way soon.¹ If you’re not seeing call validation on those devices when you accept their latest software update, you don’t have to wait. You can download the AT&T Call Protect app, or turn on the service from your account settings in myAT&T.
- AT&T Phone digital home phone users can opt-in to get AT&T Digital Phone Call Protect and call validation. Just go to your account settings on myAT&T and turn it on.
- Validation displays will be added to more mobile devices in the new year.
- Finally, a “valid number” display helps fight against bad guys, but it can never guarantee an individual caller is a good guy. Consumers should always use their best judgement when answering calls from strangers.

See, e.g., RQ-ATT0000051-RQ-ATT0000053 (https://about.att.com/story/2019/att_tmo_call_authentication.html).

AT&T* and T-Mobile today began rollout of cross-network call authentication based on SHAKEN/STIR standards – another big step toward protecting consumers from unwanted robocalls.

SHAKEN/STIR technology lets consumers know that an incoming call is really coming from the number listed on the caller ID display – not a spoofed robocall or scammer. While authentication won’t solve the problem of unwanted robocalls by itself, it is a key step toward giving customers greater confidence and control over the calls they answer.

For example, a call that is illegally “spoofed” – or shows a faked number – will fail the SHAKEN/STIR Caller ID verification and will not be marked as verified. By contrast, verification will confirm that a call is really coming from the identified number or entity. More calls will be verified over time as more device providers participate, and as more network providers implement the standards.

The FCC has recommended SHAKEN/STIR standards to digitally validate phone calls. The acronym stands for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR).

For more information on all the ways AT&T is protecting customers, visit https://about.att.com/story/2019/att_call_protect.html and <https://att.com/CyberAware>.

Caller identification authentication and verification technology, including without limitation STIR/SHAKEN, is technology configured to and/or used to, among other functions, detect spoofed phone calls. *See, e.g.,* RQ-ATT0000035-RQ-ATT0000041 (<https://www.att.com/security/>); RQ0001970 (<https://sti-ga.atis.org/resources/>).

	ATIS STANDARD ATIS-1000074-E -- SIP Forum TWG-10-E ATIS Standard on – Signature-based Handling of Asserted information using toKENs (SHAKEN) 1 Scope & Purpose 1.1 Scope This document is intended to provide telephone service providers with a framework and guidance on how to utilize Secure Telephone Identity (STI) technologies toward the validation of legitimate calls and the mitigation of illegitimate spoofing of telephone identities on IP-based service provider voice networks (also to be referred to as Voice over Internet Protocol [VoIP] networks). The primary focus of this document is on the format of STI claims, the mapping of these claims to SIP (RFC 3261), and the authentication and verification functions. 1.2 Purpose Using the protocols defined in ~~draft-ietf-stir-rfc4474bis~~RFC 8224 and ~~draft-ietf-stir-passport~~RFC 8225, this document defines the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework. This framework is targeted at telephone service providers delivering phone calls over VoIP, and addresses the implementation and usage of the IETF STIR Working Group protocols and the architecture and use of STI-related X.509-based certificates (RFC 5280). It also discusses the general architecture of service provider authentication and verification services. Finally, it provides high level guidance on the use of positive or negative verification of the signature to mitigate illegitimate telephone identity in general. Illegitimate Caller ID spoofing is a growing concern for North American telephone service providers and their customers. There are many Caller ID spoofing mechanisms, and illegitimate spoofing can evolve to evade mitigation techniques. Service provider solutions must therefore be flexible to respond to evolving threats in much the same way as cybersecurity solutions. In addition, the integration of new technologies into established VoIP networks imposes many interoperability and interworking challenges. As a result, this document is a baseline document on the implementation of the protocol-related requirements for STI. The objective is to provide a baseline that can evolve over time, incorporating more comprehensive functionality and a broader scope in a backward compatible and forward looking manner.
28[a] receiving information pertaining to a call initiated by a calling device, the information	The Accused Instrumentalities comprise computer instructions for receiving information pertaining to a call initiated by a calling device, the information pertaining to the call including: (1) a value generated based at least in part on information associated with the calling device, and (2) a score

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

pertaining to the call including: (1) a value generated based at least in part on information associated with the calling device, and (2) a score generated for the calling device, the score indicating a validity of a phone number;	generated for the calling device, the score indicating a validity of a phone number. For example, the value generated based at least in part on information associated with the calling device can include a device fingerprint, device information (e.g., make, model, serial number, operating system version, application information, or other identifying information of a device), customer account information, location information, or other information associated with the device. Furthermore, the score, which is generated for the calling device, indicates a validity of the phone number and is used to convey assurance or failure to confirm to the callee associated with the call. As one example, the received information pertaining to the call includes a score generated for the calling device, the score indicating a validity of a phone number. The score generated for the calling device may be scored from Defendants, a third party (e.g. Hiya), or some combination thereof. The score can be generated by one or more machine learning algorithms. <i>See e.g.</i>, https://work.hiya.com/adaptive-ai-ebook
---	--

Adaptive AI: A Proactive Strategy for Stopping Scam and Fraud Calls

Adaptive AI is an innovative new feature of Hiya Protect, a proprietary call protection service used by carriers, distribution partners and the Hiya mobile app.

Unlike other capabilities on the market today, Adaptive AI uses machine learning to proactively hunt and shut down scam campaigns. With the ability to stay ahead of scammers, Adaptive AI works in real-time, without the need for human intervention or any updating of existing AI models.

For example, the value generated based at least in part on information associated with the calling device can include a device fingerprint, device information (e.g., make, model, serial number, operating system version, application information, or other identifying information of a device), customer account information, location information, caller or callee number, or other information associated with the device and upon which (or upon verification of which) a security determination is in part based. The value generated based at least in part on information associated with the calling device may be generated from Defendants, a third party (e.g., Hiya), or some combination thereof.

See ATT-RQ_0000042, -43, -44 (evidencing device specific data, device settings, installed applications e.g., ActiveArmor, system or application software versions (e.g., “Device OS”, “ActiveArmor Version Information”), contact list data (TN from Device Address Book), or other

data associated with the calling device is stored and shared with AT&T’s “Vendor/Partner Hiya”). These values are used to generate a score to indicate a validity of a phone number. That score is used in the process of conveying assurance or failure to confirm for intra- and inter- network calls.

Active Armor Data Elements

As part of the Active Armor Robocall mitigation program, data elements related to calling are shared with our Vendor/Partner Hiya. Note that Hiya’s usage and management of these data elements is under written agreement with AT&T.

AT&T GFMO (Global Fraud Management Office) and AT&T CDO (Chief Data Office) each provide a set of per-Number data elements. AT&T CTS/PRS uses an API to provide per-Call data elements. There are additional data elements that are under investigation to determine if they will have value in Robocall Mitigation.

The following is a listing of each data element, by data source. See attached spreadsheet for more details.

AT&T CTS/PRS**Call Direction Response API (Per Call Basis)**

callEventNotification
 notificationType
 eventDescription
 correlationId
 callingParticipant
 callingParticipantName
 callingParticipantAlternate
 calledParticipant
 callingParticipantPrivacy
 callSessionIdentifier
 addressDirection:
 originatorTasId:
 callingParticipantAccessNetworkInfo
 callbackData
 link

 action
 actionToPerform
 displayName
 routingAddress
 decisionId
 displayAddress
 callInfo

These are additional Parameters Call Direction Response API (CR 245)

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

CTN (including AT&T/FN/Cricket customers)

Service tier (like Basic vs. Advanced)

Service Tags:

- FirstNet
- CRU
- COU
- Customers who have rate-plan-included Advanced service.
- Cricket
- Prepaid
- Wireless Home Phone

ActiveArmor Application Data

TN from Device Address Book - Hashed (shared only with explicit subscriber consent)

Device OS

ActiveArmor Version Information

The value generated based at least in part on information associated with the calling device may be generated from Defendants, a third party (e.g., Hiya), or some combination thereof.

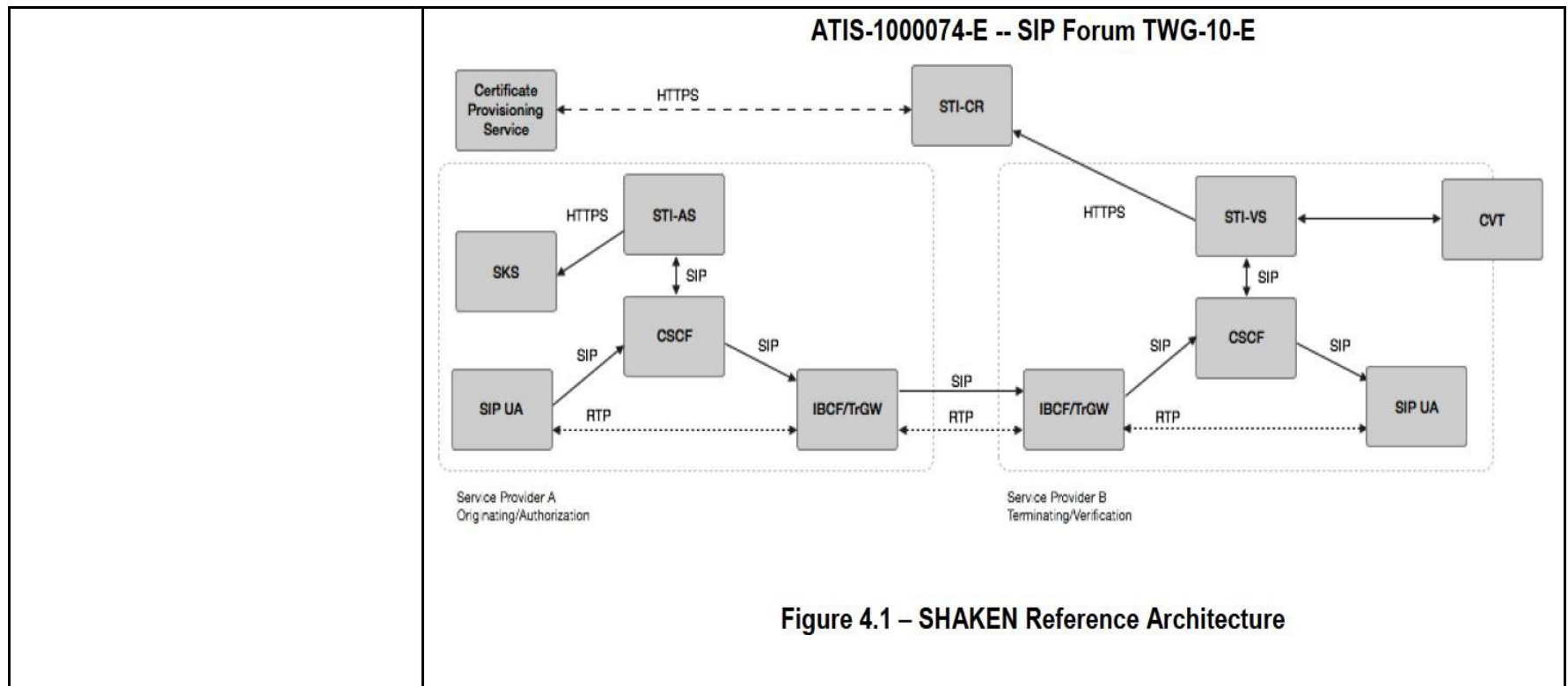
For example, Enterprise Caller Scoring is a score generated for the calling device that indicates the validity of a phone number. *See, e.g., Enterprise Caller Scoring - Stop spammers no matter what phone numbers they use*, Hiya Protect, RQ-ATT0000286-RQ-ATT0000291 (<https://www.hiya.com/products/enterprise-caller-scoring>):

How it Works

Enterprise Caller Scoring is a new layer of Hiya's Adaptive AI that stops number rotation — the practice of switching phone numbers to avoid spam detection — from being effective on mobile networks.

Like a credit agency for enterprise callers, Enterprise Caller Scoring assesses incoming calls based on the calling enterprise's history across all the numbers they own. It can identify the calling enterprise's reputation for more than 150 million enterprise phone numbers in the US — even phone numbers that haven't yet built a calling history. An enterprise's reputation continuously evolves based on behavior and is automatically recognized across all their numbers.

	<i>See also</i> Michelle Wallace, <i>How Hiya’s Proprietary Adaptive AI Stops Phone Spam</i>, Hiya Protect, https://blog.hiya.com/how-hiyas-proprietary-adaptive-ai-stops-phone-spam. Both the value and the score generated for the calling device may be generated by Defendants’ systems, a third party (e.g. Hiya) at Defendant’s request or direction, or some combination thereof. The value and score can be used to detect spoofed, spam and/or fraudulent phone calls. As another example, the Accused Instrumentalities receive information pertaining to a call initiated by a calling device. <i>See, e.g.</i>, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/); RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As another example, Call Protect, ActiveArmor, and/or the ActiveArmor mobile application use a verification service within Defendants, a third party (e.g., Hiya), or a combination thereof. As another example, STIR/SHAKEN technology comprises a verification service provider (STI-VS). <i>See, e.g.</i>, RQ0001970 (https://sti-ga.atis.org/resources/).
--	--



This SHAKEN reference architecture includes the following elements:

- SIP UA – The SIP User Agent authenticated by the service provider network. When the SIP UA is under direct management control of the telephone service provider, the service provider network can assert the calling party identity in originating SIP INVITE requests initiated by the SIP UA.
- IMS/Call Session Control Function (CSCF) – This component represents the SIP registrar and routing function. It also has a SIP application server interface.
- Interconnection Border Control Function (IBCF)/Transition Gateway (TrGW) – This function is at the edge of the service provider network and represents the Network-to-Network Interface (NNI) or peering interconnection point between telephone service providers. It is the ingress and egress point for SIP calls between providers.
- Authentication Service (STI-AS) – The SIP application server that performs the function of the authentication service defined in ~~draft-ietf-stir-rtc4474bis~~[RFC 8224](#). It should either itself be highly secured and contain the Secure Key Store (SKS) of secret private key(s) or have an authenticated, Transport Layer Security (TLS)-encrypted interface to the SKS that stores the secret private key(s) used to create PASSporT signatures.
- Verification Service (STI-VS) – The SIP application server that performs the function of the verification service defined in ~~draft-ietf-stir-rtc4474bis~~[RFC 8224](#). It has an Hypertext Transfer Protocol Secure (HTTPS) interface to the Secure Telephone Identity Certificate Repository that is referenced in the Identity header field to retrieve the provider public key certificate.
- Call Validation Treatment (CVT) – This is a logical function that could be an application server function or a third party application for applying anti-spoofing mitigation techniques once the signature is positively or negatively verified. The CVT can also provide information in its response that indicates how the results of the verification should be displayed to the called user.
- SKS – The Secure Key Store is a logical highly secure element that stores secret private key(s) for the authentication service (STI-AS) to access.
- Certificate Provisioning Service – A logical service used to provision certificate(s) used for STI.
- Secure Telephone Identity Certificate Repository (STI-CR) – This represents the publically accessible store for public key certificates. This should be an HTTPS web service that can be validated back to the owner of the public key certificate.

As one example, within the Accused Instrumentalities, the received information pertaining to the call includes a value generated based at least in part on information associated with the calling device. For example, the SIP Identity header is generated from information associated with the device. *See, e.g.*, RQ0001970 (<https://sti-ga.atis.org/resources/>). As one example, the SIP Identity header comprises the Personal Assertion Token (PASSporT), which is a value generated based at least in part on information associated with the calling device. *See, e.g.*, RQ0001970 (<https://sti-ga.atis.org/resources/>).

4.1 STIR Overview

The documents ~~ietf-stir-rfc4474bis~~[RFC 8224](#) and ~~ietf-stir-passport~~[RFC 8225](#) define a set of protocol level tools that can be used in Session Initiation Protocol (SIP) for applying digital signatures to the Caller ID or telephone number of the calling party.

4.1.1 Personal Assertion Token (PASSporT) ~~Token~~

The document ~~ietf-stir-passport~~[RFC 8225](#) defines a token-based signature that combines the use of JavaScript Object Notation (JSON) Web Tokens, JSON Web Signatures, and X.509 certificate key pairs, or Public Key Infrastructure (PKI), to create a trusted signature. The authorized owner of the certificate used to generate the signature can be validated and traced back to the known trust anchor who signed the certificate. The Personal Assertion Token (PASSporT) ~~token~~ includes a number of claims the signer of the token is asserting. The associated public certificate is used to verify the digital signature and the claims included in the PASSporT~~token~~. The public certificate is also used to validate the entity that signed the token through a Service Provider Identifier (SPID), as defined in ~~ietf-stir-certificates~~[RFC 8226](#). The validated claims and the validated identity of the entity signing the claims can both be used to determine the level of trust in the originating entity and their asserted calling party information. Call blocking applications or other mitigation techniques could use the information over time to determine "reputation" of the entity signing the token, which could provide further input to determine the level of trust for the calling party information. Note that PASSporT~~s~~~~tokens~~ and signatures themselves are agnostic to network signaling protocols but are used in ~~draft-ietf-stir-rfc4474bis~~[RFC 8224](#) to define specific SIP usage as described in the next section.

See also J. Peterson et al., *Authenticated Identity Management in the Session Initiation Protocol (SIP)*, Internet Engineering Task Force (Feb. 2018), RQ0001971-RQ0002016 (<https://tools.ietf.org/html/rfc8224>).

Step 4: Populate and Add the Identity Header

Subsequently, the authentication service MUST form a PASSporT object and add a corresponding Identity header field to the request containing either the full or compact form of PASSporT. For the baseline PASSporT header (headers containing no "ppt" parameter), this follows the procedures in [Section 4](#); if the authentication service is using an alternative "ppt" format, it MUST add an appropriate "ppt" parameter and follow the procedures associated with that extension (see [Section 9](#)). After the Identity header field has been added to the request, the authentication service MUST also add an "info" parameter to the Identity header field. The "info" parameter contains a URI from which the authentication service's credential can be acquired; see [Section 7.3](#) for more on credential acquisition.

6.2. Verifier Behavior

This document specifies a logical role for SIP entities; this role is called a verification service, or verifier. When a verifier receives a SIP message containing one or more Identity header fields, it inspects the signature(s) to verify the identity of the originator of the message. The results of a verification are provided as input to an authorization process that is outside the scope of this document.

See also RQ0002017-RQ0002041 (<https://datatracker.ietf.org/doc/html/rfc8225>).

PASSport specifically uses this token format and defines claims that convey the identity of the origination and destination of personal communications. The primary value asserted in a PASSport object is the originating identity representing the identity of the calling party or the initiator of a personal-communications session. The signer of a PASSport object may or may not correspond to the originating identity. For a given application's use or using protocol of PASSport, the creation of the PASSport object is performed by an entity that is authoritative to assert the caller's identity. This authority is represented by the certificate credentials and the signature, and the PASSport object is created and initiated to the destination(s) per the application's choice of authoritative point(s) in the network. For example, the PASSport object could be created at a device that has authenticated with a user or at a network entity with an authenticated trust relationship with that device and its user. Destination identities represent the intended destination of the personal communications, i.e., the identity(s) being called by the caller. The destination point or points determined by the application need to have the capability to verify the PASSport and the digital signature. The PASSport-associated certificate is used to validate the authority of the originating signer, generally via a certificate chain to the trust anchor for that application.

Best Practices for Obtaining Mobile Device Identifiers for Mobile Device Theft Prevention (MDTP)

Alliance for Telecommunications Industry Solutions

Approved October 2015

Abstract

This specification defines best practices for obtaining the device identifiers (e.g., International Mobile Equipment Identity [IMEI]) from mobile devices even if the mobile device is locked or disabled. This best practices specification was developed in response to Recommendation 1.5 of the December 4, 2014 Federal Communications Commission (FCC) Technological Advisory Council (TAC) report on Mobile Device Theft Prevention (MDTP).

5.2.4 Origination Identifier (“origid”)

In addition to attestation, the unique origination identifier (“origid”) is defined as part of SHAKEN. This unique origination identifier should be a globally unique string corresponding to a Universally Unique Identifier (UUID) (RFC 4122).

The purpose of the unique origination identifier is to assign an opaque identifier corresponding to all or part of the originating service provider’s network (data centers, IBCF nodes, access networks, IMS core complexes, etc.) ~~initiated calls themselves~~, customers, customer or interconnecting service provider nodes, classes of customer devices, or other groupings that a service provider might want to use to indicate common call sources for determining things such as reputation or trace back identification of customers or gateways.

The origid is not intended to directly expose or be reverse-engineered to a customer or service provider identity, but it should be useful for analytics purposes in remote networks and traceback within the originating service provider network.

Best practices will specify when it is appropriate to use groupings less-granular than per-customer, customer device or node, or interconnecting service provider or interconnecting service provider node for origination identifier marking. Where origination identifier granularity is at the customer level or finer, best practices should also cover methods to protect the privacy of individual customers whose identity might be deduced through calling patterns. ~~For Full Attestation, in general, a single identifier will be used as part of the certificate representing direct service provider initiated calls on its VoIP network. A service provider may, for example, also choose to have a pool of identifiers to differentiate geographic regions or classes of customers. Best practices will likely develop as trace back and illegitimate call identification practices evolve.~~

~~For Partial Attestation, a single identifier per customer is required in order to differentiate calls both for trace back and reputation segmentation so that one customer’s reputation doesn’t affect other customer’s or the service provider’s call reputation. A service provider may choose to be more granular (e.g., per node per customer) depending on its size and classes of services that the service provider offers.~~

~~For Gateway Attestation, best practices will dictate that the “origid” should be sufficiently granular to identify the originating node or trunk to allow for trace back identification and reputation scoring.~~

AT&T further discloses that the Accused Instrumentalities receive and use the following information associated with the calling device. *See, e.g.,* RQ-ATT0000070-RQ-ATT0000086 (<https://about.att.com/privacy/privacy-notice.html>):

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

	The information we collect x To better run our business, we collect information about you, your equipment and how you use our products and services. This can include: • Account information. You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including Customer Proprietary Network Information. • Equipment information. We collect information about equipment on our network like the type of device you use, device ID, and phone number. • Network performance. We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working. • Location information. Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites. • Web browsing and app information. We automatically collect a variety of information which may include time spent on websites or apps, website and IP addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information. • Biometric information. Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our Biometric Information Privacy Notice. • Third-party information. We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T.
--	--

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

	How we use your information × We rely on the information we collect to support our business functions, power our services and improve your experience, such as when we: • Combine it with the information from testing and running our network to determine which products and services better meet the needs of our customers. • Provide our products and services. • Contact you. • Improve your experience and safety. This includes verifying your identity, detecting and preventing fraud, protecting your financial accounts, authorizing transactions and assisting your interactions with customer care. • Improve and protect our network. • Use it to help understand which additional products and services may interest you and others. (We don't access or use the content of your texts, emails or calls for this or any other marketing and advertising.) • Design and deliver advertising, marketing and promotional campaigns to you and others – and measuring their effectiveness (See your choices). • Use it for billing, collection, and protection of our property and legal rights. • Prevent and investigate security issues, illegal activities, and violations of our terms and conditions. • Conduct research and create aggregated reports – reports that offer insights about groups of customers, but not individuals (we do not attempt to re-identify individuals in aggregated reports). <i>See also AT&T ActiveArmor Mobile Security Application and Service, AT&T, RQ-ATT0000139-RQ-ATT0000150 (https://www.att.com/legal/terms.activeArmorMobileSecurity.html):</i>
--	--

	In order to perform the functions of the Service including but not limited to its Call Features, AT&T may use and/or disclose or allow the disclosure to our third-party vendor(s) of Your personal information, including without limitation mobile number, contacts/address book in order to populate detail in the call detail screen, the presence or absence of calling party phone numbers in your Device address book, and App usage information, such as which numbers you report and/or manually block within the App, as factors to determine which callers are suspected fraud and spam. The contact names and phone numbers in your Device address book are not shared for any purpose other than improving your experience with the App by helping you to recognize known callers. 3.2 Consent for Information Disclosure in Connection with Data Features The Service includes the following data security and related features: Device Security Alerts, Data Breach Alerts, Public Wi-Fi Protection (VPN & Wi-Fi Alerts), Identity Monitoring, Reverse Number Lookup, Safe Browsing, and Device Theft Alerts (collectively “Data Features”) In order to perform the functions and to improve the effectiveness of the Service including but not limited to its Data Features for all users, AT&T, its pertinent suppliers and their subsidiaries, agents and subcontractors may collect, maintain, process, use, and disclose diagnostic, technical, usage and related information including, but not limited to, information about: • the type of Device You are using and the operating system You are running; • Your applicable wireless network provider/carrier; • the applications and files present on Your Device and SD memory card; • the results of any scans performed by the App; and • actions You take as a result of any virus or malware notifications. We also may collect information about how the App and any associated Service applications behave on Your Device and the network services with which applications installed on Your Device communicate in order to determine if any applications are behaving maliciously (for example, is an application accessing Your address contacts, sending premium-rate text messages that charge money to Your wireless bill, or communicating with a server known to host phishing websites). As one example, within the Accused Instrumentalities, the received information pertaining to the call includes a score generated for the calling device, the score indicating a validity of a phone number. For example, the score generated for the calling device comprises and/or has as an input or signal, among other inputs and/or signals, an indication of the attestation level associated with the calling device and indicates a validity of a phone number, but the score is not limited to the A or B or C attestation level. <i>See, e.g.</i>, RQ0001970 (https://sti-ga.atis.org/resources/).
--	---

5.2.3 Attestation Indicator (“attest”)

The “attest” claim allows the originating service provider that is populating an Identity header to clearly indicate the information it can vouch for regarding the origination of the call.

~~This indicator allows for both identifying the service provider that is vouching for the call as well as clearly indicating what information the service provider is attesting to.~~

In the SHAKEN framework we define the following three levels of attestation:

A. Full Attestation: The signing provider shall satisfy all of the following conditions:

- Is responsible for the origination of the call onto the IP-based service provider voice network.
- Has a direct authenticated relationship with the customer and can identify the customer.
- Has established a verified association with the telephone number used for the call.

NOTE 1: The signing provider is asserting that their customer can “legitimately” use the number that appears as the calling party (i.e., the Caller ID). The legitimacy of the telephone number(s) the originator of the call can use is subject to signer-specific policy, but could use mechanisms such as the following:

- The number was assigned to this customer by the signing service provider.
- This number is one of a range of numbers assigned to an enterprise or wholesale customer.
- The signing service provider has ascertained that the customer is authorized to use a number (e.g., by business agreement or evidence the customer has access to use the number). This includes numbers assigned by another service provider.
- The number is not permanently assigned to an individual customer but the signing provider can track the use of the number by a customer for certain calls or during a certain timeframe.

NOTE 2: Ultimately it is up to service provider policy to decide what constitutes “legitimate right to assert a telephone number” but the service provider’s reputation may be directly dependent on how rigorous they have been in making this assertion.

B. Partial Attestation: The signing provider shall satisfy all of the following conditions:

- Is responsible for the origination of the call onto ~~its~~ the IP-based service provider voice network.
- Has a direct authenticated relationship with the customer and can identify the customer.
- Has NOT established a verified association with the telephone number being used for the call.

9

ATIS-1000074-E -- SIP Forum TWG-10-E

NOTE: By populating this value, the service provider attests that it can trace the source of the call to a customer for policy enforcement purposes~~When partial attestation is used, each customer will have a unique origination identifier created and managed by the service provider, but the intention is that it will not be possible to reverse engineer the identity of the customer purely from the identifier or signature. As described in section 5.2.4, the unique origination identifier allows data analytics to establish a reputation profile and assess the reliability of information asserted by the customer assigned this unique identifier. The identifier also provides a reliable mechanism to determine the customer for forensic analysis or legal action where appropriate.~~

[The verifier validates that the PASSporT ~~token~~ provided in the Identity header of the INVITE includes all of the baseline claims, as well as the SHAKEN extension claims. The verifier shall also follow the ~~draft-ietf-stir-#c4474bis~~ RFC 8224-defined verification procedures to check the corresponding date, originating identity (i.e., the originating telephone number) and destination identities (i.e., the terminating telephone numbers), with the restrictions specified in this section.

	C. Gateway Attestation: The signing provider shall satisfy all of the following conditions: ~~Is the entry point of the call into its VoIP network.~~ - Has no relationship with the initiator of the call (e.g., international gateways). ~~NOTE: The token will provide a unique origination identifier of the node in the “origid” claim. (The signer is not asserting anything other than “this is the point where the call entered my network”.)~~ <u>NOTE: The signer/originating service provider should be able to trace a call to an interconnecting service provider and/or peer node for traceback or policy enforcement purposes. Gateway attestation may also be used when the STI-AS does not have sufficient information for determining that A or B attestation applies even when the call was received at a customer interface.</u> For the PASSporT extension claim, the “attest” key value pair shall be set to uppercase characters “A”, “B”, or “C” corresponding to the appropriate attestation defined above. An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
28[b] performing a security determination based at least in part on the score generated for the calling device, and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device; and	The Accused Instrumentalities comprise computer instructions for performing a security determination based at least in part on the score generated for the calling device, and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device. The Accused Instrumentalities perform and/or are capable of performing a security determination based at least in part on the score generated for the calling device and at least in party by verifying the value included in the information pertaining to the call, from Defendants, a third party (e.g. Hiya), or some combination thereof. <i>See e.g.</i>, https://work.hiya.com/adaptive-ai-ebook

Adaptive AI: A Proactive Strategy for Stopping Scam and Fraud Calls

Adaptive AI is an innovative new feature of Hiya Protect, a proprietary call protection service used by carriers, distribution partners and the Hiya mobile app.

Unlike other capabilities on the market today, Adaptive AI uses machine learning to proactively hunt and shut down scam campaigns. With the ability to stay ahead of scammers, Adaptive AI works in real-time, without the need for human intervention or any updating of existing AI models.

For example, the value generated based at least in part on information associated with the calling device can include a device fingerprint, device information (e.g., make, model, serial number, operating system version, application information, or other identifying information of a device), customer account information, location information, caller or callee number, or other information associated with the device and upon which (or upon verification of which) a security determination is in part based. The value generated based at least in part on information associated with the calling device may be generated from Defendants, a third party (e.g., Hiya), or some combination thereof and is verified as part of the security determination when deciding to connect, convey assurance of the callee, convey a failure to confirm the callee, and/or refuse to connect the initiated call.

For example, Defendant's Robocall mitigation system performs a security determination based at least in part on the score generated for the calling device, and at least in part by verifying the value. *See* ATT-RQ 0000042, -43, -44 (evidencing device specific data, device settings, installed

applications e.g., ActiveArmor, system or application software versions (e.g., “Device OS”, “ActiveArmor Version Information”), contact list data (TN from Device Address Book), or other data associated with the calling device is stored and shared with AT&T’s “Vendor/Partner Hiya”). These values are used, along with one or more scores to determine the validity of a phone number. Furthermore, the score and value are used in the process of conveying assurance or failure to confirm for intra- and inter- network calls.

Active Armor Data Elements

As part of the Active Armor Robocall mitigation program, data elements related to calling are shared with our Vendor/Partner Hiya. Note that Hiya’s usage and management of these data elements is under written agreement with AT&T.

AT&T GFMO (Global Fraud Management Office) and AT&T CDO (Chief Data Office) each provide a set of per-Number data elements. AT&T CTS/PRS uses an API to provide per-Call data elements. There are additional data elements that are under investigation to determine if they will have value in Robocall Mitigation.

The following is a listing of each data element, by data source. See attached spreadsheet for more details.

AT&T CTS/PRS**Call Direction Response API (Per Call Basis)**

callEventNotification
 notificationType
 eventDescription
 correlationId
 callingParticipant
 callingParticipantName
 callingParticipantAlternate
 calledParticipant
 callingParticipantPrivacy
 callSessionIdentifier
 addressDirection:
 originatorTasId:
 callingParticipantAccessNetworkInfo
 callbackData
 link

 action
 actionToPerform
 displayName
 routingAddress
 decisionId
 displayAddress
 callInfo

These are additional Parameters Call Direction Response API (CR 245)

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

CTN (including AT&T/FN/Cricket customers)

Service tier (like Basic vs. Advanced)

Service Tags:

- FirstNet
- CRU
- COU
- Customers who have rate-plan-included Advanced service.
- Cricket
- Prepaid
- Wireless Home Phone

ActiveArmor Application Data

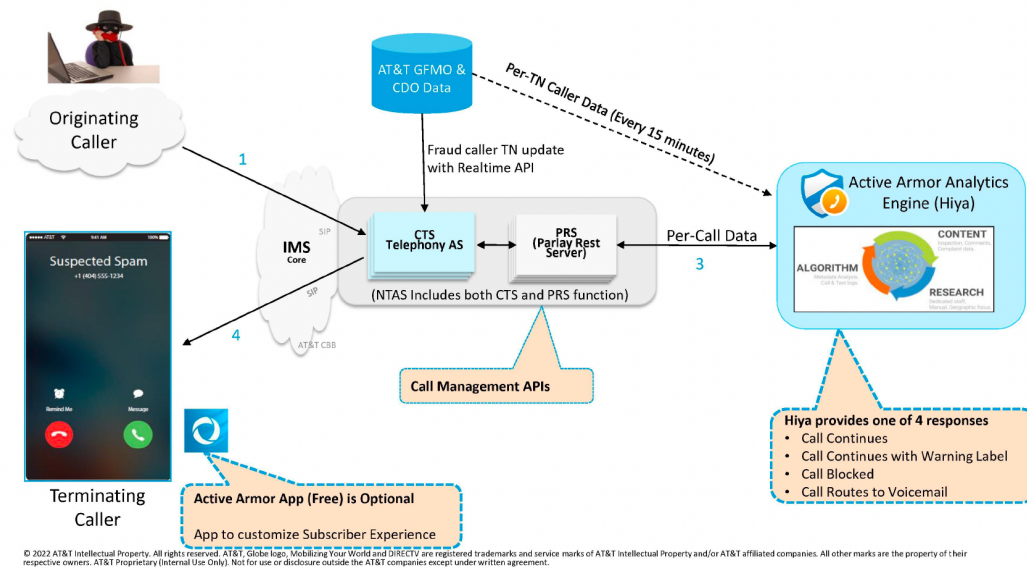
TN from Device Address Book - Hashed (shared only with explicit subscriber consent)

Device OS

ActiveArmor Version Information

See, e.g., ATT-RQ_0000045 showing that Hiya provides at least one of 4 responses – namely, “Call Continues,” “Call Continues with Warning Label”, “Call Blocked” or “Call Routes to Voicemail” (e.g., whether or not the call should be connected or blocked).

AT&T Active Armor (Call Protect) – High Level Architecture



© 2022 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T companies except under written agreement.

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

ATT-RQ_0000045

As another example, Enterprise Caller Scoring is a score generated for the calling device that indicates the validity of a phone number. *See, e.g., Enterprise Caller Scoring - Stop spammers no matter what phone numbers they use, Hiya Protect, RQ-ATT0000286-RQ-ATT0000291* (<https://www.hiya.com/products/enterprise-caller-scoring>):

How it Works

Enterprise Caller Scoring is a new layer of Hiya's Adaptive AI that stops number rotation — the practice of switching phone numbers to avoid spam detection — from being effective on mobile networks.

Like a credit agency for enterprise callers, Enterprise Caller Scoring assesses incoming calls based on the calling enterprise's history across all the numbers they own. It can identify the calling enterprise's reputation for more than 150 million enterprise phone numbers in the US — even phone numbers that haven't yet built a calling history. An enterprise's reputation continuously evolves based on behavior and is automatically recognized across all their numbers.

See also <https://blog.hiya.com/how-hiyas-proprietary-adaptive-ai-stops-phone-spam>.

As another example, Accused Instrumentalities perform a security determination based at least in part on the SIP Identity header. The SIP Identity header is based at least in part on the score generated

for the calling device, and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device. *See, e.g.*, RQ0001970 (<https://sti-ga.atis.org/resources/>).

As one example, the Accused Instrumentalities perform a security determination based at least in part on a public certificate, which is verifying the value comprised in the SIP Identity header included in the information pertaining to the call initiated by the calling device. As one example, the value is the Personal Assertion Token (PASSporT).

[The verifier validates that the PASSporT ~~token~~ provided in the Identity header of the INVITE includes all of the baseline claims, as well as the SHAKEN extension claims. The verifier shall also follow the ~~draft-ietf-stir-fc4474bis~~ RFC 8224-defined verification procedures to check the corresponding date, originating identity (i.e., the originating telephone number) and destination identities (i.e., the terminating telephone numbers), with the restrictions specified in this section.

As one example, the Accused Instrumentalities perform a security determination based at least in part on the attestation level. The attestation level is based at least in part on the score generated for the calling device and at least in part by verifying the value included in the information pertaining to the call initiated by the calling device. *See, e.g.*, RQ0001970 (<https://sti-ga.atis.org/resources/>).

Use of standardized cryptographic digital signatures to validate the originator of a signed identity can provide a verifiable mechanism to identify the authorized originator of a call into the VoIP network with non-repudiation. Further, the use of an assigned attestation indicator and a unique origination identifier depending on how and where the call is originated in the VoIP network represents the originating signer’s ability to vouch for the accuracy of the source of origin of the call. For example, if the service provider has an authenticated direct relationship with the origination of the call, this attestation is categorized differently than calls that are originated from different networks or gateways that the service provider may have received from an unauthenticated network or that are

3

ATIS-1000074-E -- SIP Forum TWG-10-E

unsigned. Verifiers of signatures will use these attestations as information to provide trace back mechanisms, as well as information to feed into any call spam identification solution enabled on behalf of their customer.

5.2.2 PASSporT Extension “shaken”

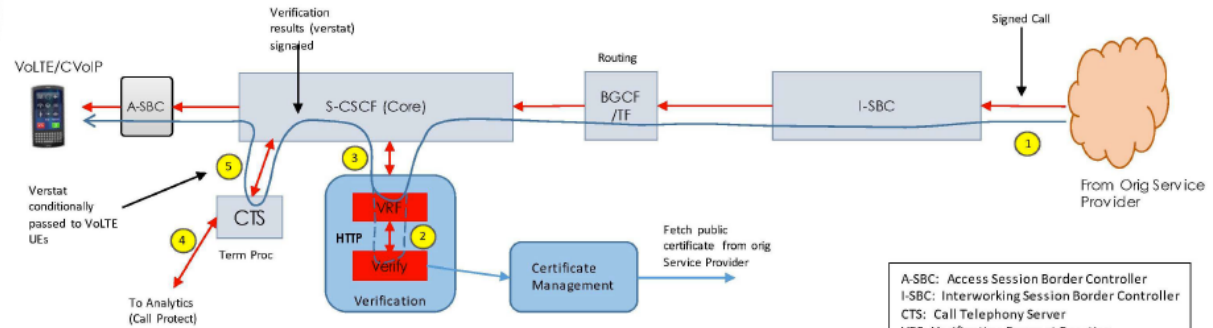
The base PASSporT set of claims cover the assertion of the originating telephone number along with date and destination telephone numbers to avoid replay attacks using valid Identity header fields. draft-ietf-stir-passport-shaken defines~~This section will detail a specific~~ the “shaken” extension to ~~the~~ PASSporT to cover the following requirements of SHAKEN. The ~~SHAKEN~~ “shaken” extension to PASSporT shall be implemented with all extension claims as part of the signed PASSporT ~~token~~.

1. The ability to provide an attestation indicator for the context of how the call was originated.
2. The ability to provide a unique originating identifier, as described in Section 5.2.4, that can serve as an opaque indication of where in the originating service provider’s network the call was originated. ~~This identifier shall be globally unique and consistent so it can be used in analytics for tracking the reputation of a particular originating service and could also be used for any traceback efforts if a particular originator is a consistent or pervasive “bad actor”.~~

The PASSporT “shaken” extension shall include both an attestation indicator (“attest”), as described in section 5.2.3 and an origination identifier (“origid”) as described in section 5.2.4. The SHAKEN PASSporT ~~token~~ would have the form given in the example below:

As another example, intra-network calls may be treated differently from inter-network calls. The attestation level of a call may be included within a verstat (verification indicator) tag, or other header. *See e.g., ATT-RQ-466, 467.*

Inter-Network SHAKEN Flows (ATT terminated)



1. Signed call is received from an originating carrier that supports SHAKEN. Terminating S-CSCF detects the received Identity header and sends the call to the VRF.
2. The VRF formulates the HTTP verification request and sends the request to the Verification Server.
3. The verification results are returned and signaled in the "verstat" parameter (contained in PAI/From headers).
4. Verstat is used by analytics (e.g. Call Protect) as an input to reputation scoring.
5. Verstat is conditionally passed to terminating VolTE UE and UE uses this information to influence the calling number/name display information. For CVoIP, term CTS modifies the Calling Number to include SHAKEN verification results.

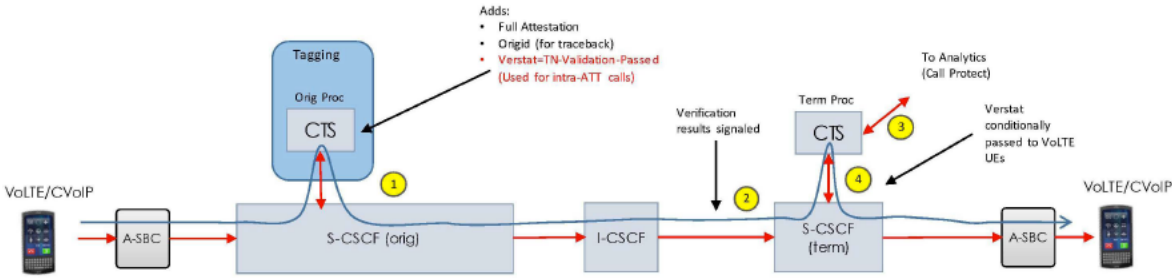
AT&T Proprietary and Confidential

This document and information contained therein is not for use or disclosure outside of AT&T

RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

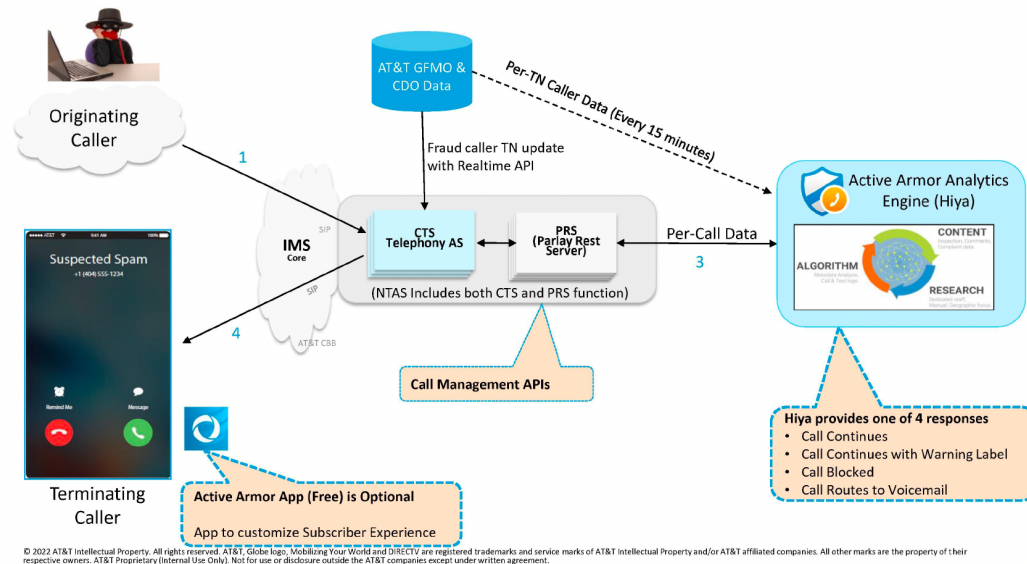


ATT-RQ_0000466

	Intra-AT&T SHAKEN Flows  The diagram illustrates the Intra-AT&T SHAKEN Flows. It shows a call path starting from a VoLTE/CVoIP device, passing through an A-SBC, then an S-CSCF (orig), then an I-CSCF, then an S-CSCF (term), and finally through another A-SBC to a terminating VoLTE/CVoIP device. Key components include the Tagging process (Orig Proc CTS) and the Term Proc CTS. The flow is numbered 1 through 4, corresponding to the steps listed below. A legend box defines the acronyms: A-SBC: Access Session Border Controller, CTS: Call Telephony Server, I-CSCF: Interrogating Call Session Control Function, and S-CSCF: Serving Call Session Control Function. A list of adds (Full Attestation, OrigID (for traceback), Verstat=TN Validation-Passed (Used for intra-ATT calls)) is shown. Verification results are signaled from the I-CSCF to the Term Proc CTS. Verstat is conditionally passed to VoLTE UEs and used by analytics (e.g., Call Protect) for reputation scoring. For CVoIP, term CTS modifies the Calling Number to include SHAKEN verification results. - After originating processing is completed, CVoIP/VoLTE calls will be "tagged". - Tagging adds verstat parameter to emulate a call that was verified successfully. This is used for intra-network (ATT to ATT) calls. - Intra-ATT calls are not "signed". - The emulated verification result (verstat) is passed to CTS. - Verstat is used by analytics (e.g. Call Protect) as an input to reputation scoring. - Verstat is conditionally passed to terminating VoLTE UE and UE uses this information to influence the calling number/name display information. For CVoIP, term CTS modifies the Calling Number to include SHAKEN verification results. AT&T Proprietary and Confidential This document and information contained therein is not for use or disclosure outside of AT&T ATT-RQ_0000467
28[c] based at least in part on the security determination, performing at least one of conveying an assurance to a callee associated with the call or conveying a failure to confirm to the callee associated with the call.	The Accused Instrumentalities comprise computer instruction for, based at least in part on the security determination, performing at least one of conveying an assurance to a callee associated with the call or conveying a failure to confirm to the callee associated with the call. <i>See, e.g.,</i> ATT-RQ_0000045 (Hiya provides at least one of four responses – namely, “Call Continues,” “Call Continues with Warning Label”, “Call Blocked” or “Call Routes to Voicemail”

(e.g., whether or not the call has an assurance or a failure of an assurance)):

AT&T Active Armor (Call Protect) – High Level Architecture



RESTRICTED – OUTSIDE ATTORNEYS’ EYES ONLY

ATT-RQ_0000045

As one example, based at least in part on the security determination, the Accused Instrumentalities convey an assurance to a callee associated with the call, including but not limited to conveying a green check, “valid number,” or “[V]”, brand logos, contact/caller name, and/or otherwise providing call logs, reports, or other indications reflecting confirmation.

See, e.g., RQ-ATT0000024-RQ-ATT0000026

(https://about.att.com/story/2019/call_validation_displays.html).



*Samsung Galaxy S10, Galaxy S10+, LG V40 ThinQ and AT&T Digital Home
Phone Service Can Now Show That a Call Is Authenticated*

AT&T* has turned on its first phone displays that let you know an incoming call is really from the number appearing on Caller ID. This fights against “spoofing” of phone numbers – a trick used by many illegal robocallers.

Most AT&T customers with a Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ™ will see a special display when an incoming call has been authenticated. They will see a green checkmark and the words, “Valid Number.”

Consumers with AT&T Phone digital home phone service also can activate the feature. It will give them a “[V]” for valid number.

Phone service providers have jointly developed a technology – the SHAKEN/STIR standards – to digitally validate calls. This won’t solve the problem of unwanted robocalls by itself. But it can give consumers greater confidence and control over the calls they answer.

“This is another step to tame annoying, unwanted robocalls,” said Kevin Petersen, AT&T senior vice president, Postpaid Wireless Products. “In the coming year, we’ll continue to take more steps and put more pressure on the bad guys.”

AT&T is rolling out its SHAKEN/STIR display as part of its AT&T Call Protect service, which is being added at no charge to millions of mobility consumer lines. AT&T Call Protect blocks or labels suspected illegal and unwanted robocalls.

This strategy will give a multiplier effect to call protection: A “valid number” on an AT&T device means the incoming call has been authenticated by SHAKEN/STIR *and* passed through AT&T Call Protect screening.

Here are some other key points:

- A call that shows “valid number” has been verified and can increase your trust level. But a call without the label may still be a legitimate call. More calls will be marked with “valid number” over time, as more network providers implement SHAKEN/STIR and link to each other.
- AT&T has rolled out AT&T Call Protect automatically to many Samsung Galaxy S10, Galaxy S10+ and LG V40 ThinQ users. Others are on the way soon.¹ If you’re not seeing call validation on those devices when you accept their latest software update, you don’t have to wait. You can download the AT&T Call Protect app, or turn on the service from your account settings in myAT&T.
- AT&T Phone digital home phone users can opt-in to get AT&T Digital Phone Call Protect and call validation. Just go to your account settings on myAT&T and turn it on.
- Validation displays will be added to more mobile devices in the new year.
- Finally, a “valid number” display helps fight against bad guys, but it can never guarantee an individual caller is a good guy. Consumers should always use their best judgement when answering calls from strangers.

See, e.g., RQ-ATT0000137-RQ-ATT0000138 (<https://www.att.com/support/article/u-verse-voice/KM1235421/>):

Digital Phone Call Protect features

Here's what you get with Digital Phone Call Protect¹:

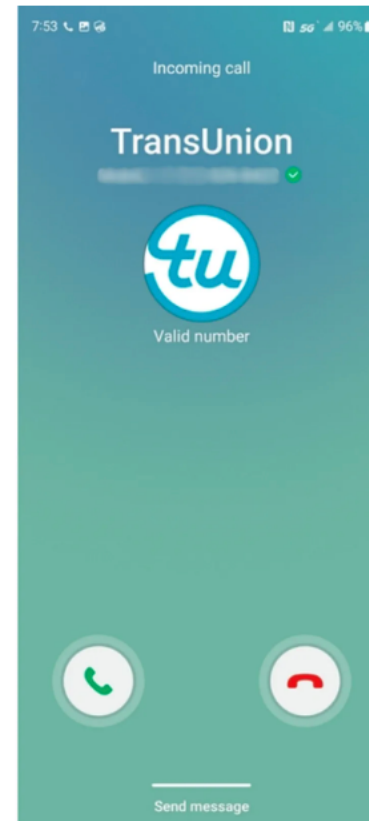
- **Call validation:** Soon you'll see a [V] on your caller ID for some calls. This means we've confirmed that the call originated from the phone registered to that number. (Remember to still be cautious when answering a call from an unknown number.)
- **Automatic fraud blocking:** Each potential fraud call gives the caller a busy signal, and the call won't go through. You can toggle this feature on or off.
- **Call blocking:** If you have a specific number you want to block, press *61 after the unwanted call to block that number.
- **Call log:** You can see detailed call log info.
- **Suspected spam call warning:** Your caller ID will show Suspected Spam and a type (Political, Nonprofit, Telemarketer, Survey, or Robocaller).

See also ATT0000088-RQ-ATT0000090 (<https://www.idropnews.com/news/fast-tech/att-will-warn-you-of-incoming-robocalls-but-not-on-iphone/125657/>):

It's worth noting that AT&T also offers call verification for iPhone users, *but it won't show up when the call is coming in.*

- To see if a number is verified on iPhone, you'll need to check your call log in the **Phone app** under **Recents**.
- Verified unknown calls will have a checkmark next to them on recent versions of iOS. This clunky method is likely to change in the future, however.

See, e.g., RQ-ATT0000091-RQ-ATT0000094 (<https://www.cnet.com/tech/mobile/at-t-adopts-new-robocall-fighting-tool-that-adds-logo-images-to-caller-id/>):



An example of a company logo that appears when a carrier uses Branded Call Display to authenticate a call.

As another example, based at least in part on the security determination, the Accused Instrumentalities convey or are configured to convey a failure to confirm to the callee the identity of the caller, including but not limited to providing, showing, alerting, labeling, or otherwise indicating potential fraud/spam indicators, “unknown caller” indicators, call logs or other reports, or any other indication of failure to confirm, and/or by not showing, alerting, labeling, or otherwise indicating “valid,” a green checkmark, “[V]”, and/or any other indication of confirmation.

See, e.g., RQ-ATT0000095-RQ-ATT0000098 (<https://forums.att.com/conversations/account-features/blocking-unknown-numbers/63b33783c1c54d548b8bbe5b>).

Hey, rehjaeger! The AT&T ActiveArmor application allows you to flag, send to voicemail, and block nuisance & fraud risk calls. You can also send unknown callers to voicemail.

To find these settings, you'll open up the AT&T ActiveArmor app then click on the phone icon named **Calls**. After, you'll scroll down until you see **Network Call Preferences**. From there, select the drop down arrow listed near **Unknown callers** and click **send to voicemail**. Keep in mind, you can only see these settings while connected to your cellular data.

To answer your question you can't personally block all unknown callers but you can automatically forward them to your voicemail.

We hope we've answered your question! Please let us know if you have additional inquiries!

Jonye, AT&T Community Specialist

See, e.g., RQ-ATT0000046-RQ-ATT0000048 (<https://about.att.com/blogs/2023/activearmor-text-blocking.html>).

- **We block all the fraud calls we can find.** And we label suspected spam calls so you can choose to answer or not. We do this for every customer on our network – more than a billion blocked or labeled calls a month.

See, e.g., RQ-ATT0000051-RQ-ATT0000053 (https://about.att.com/story/2019/att_tmo_call-authentication.html):

AT&T* and T-Mobile today began rollout of cross-network call authentication based on SHAKEN/STIR standards – another big step toward protecting consumers from unwanted robocalls.

SHAKEN/STIR technology lets consumers know that an incoming call is really coming from the number listed on the caller ID display – not a spoofed robocall or scammer. While authentication won’t solve the problem of unwanted robocalls by itself, it is a key step toward giving customers greater confidence and control over the calls they answer.

For example, a call that is illegally “spoofed” – or shows a faked number – will fail the SHAKEN/STIR Caller ID verification and will not be marked as verified. By contrast, verification will confirm that a call is really coming from the identified number or entity. More calls will be verified over time as more device providers participate, and as more network providers implement the standards.

The FCC has recommended SHAKEN/STIR standards to digitally validate phone calls. The acronym stands for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR).

For more information on all the ways AT&T is protecting customers, visit https://about.att.com/story/2019/att_call_protect.html and <https://att.com/CyberAware>.

See also RQ0001970 (<https://sti-ga.atis.org/resources/>):

The terminating network conveys the verification result to the called user by including a “verstat” parameter in the From and/or P-Asserted-Identity header fields of the INVITE request sent to the called endpoint device, as defined in [TS 24.229].

- Call Validation Treatment (CVT) – This is a logical function that could be an application server function or a third party application for applying anti-spoofing mitigation techniques once the signature is positively or negatively verified. The CVT can also provide information in its response that indicates how the results of the verification should be displayed to the called user.

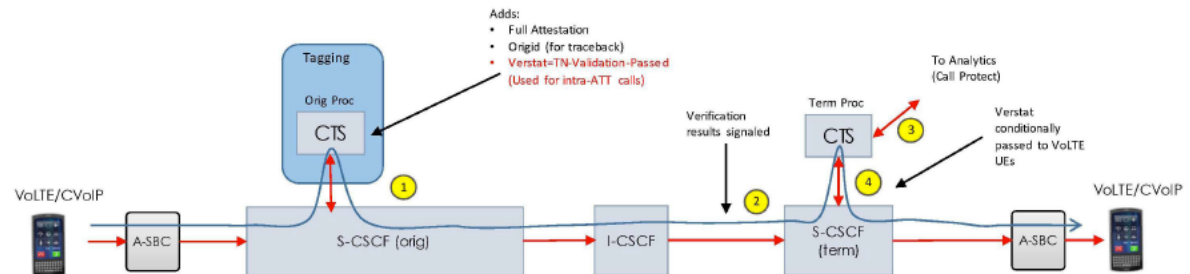
As another example, intra-network calls may be treated differently from inter-network calls. The attestation level of a call may be included within a verstat (verification indicator) tag, or other header. See e.g., ATT-RQ-466, 467.



This document and information contained therein is not for use or disclosure outside of AT&T

ATT-RQ 0000466

Intra-AT&T SHAKEN Flows



1. After originating processing is completed, CVoIP/VoLTE calls will be "tagged".
 - Tagging adds verstat parameter to emulate a call that was verified successfully. This is used for intra-network (ATT to ATT) calls.
 - **Intra-ATT calls are not "signed"**
2. The emulated verification result (verstat) is passed to CTS.
3. Verstat is used by analytics (e.g. Call Protect) as an input to reputation scoring.
4. Verstat is conditionally passed to terminating VoLTE UE and UE uses this information to influence the calling number/name display information. For CVoIP, term CTS modifies the Calling Number to include SHAKEN verification results.

A-SBC: Access Session Border Controller
 CTS: Call Telephony Server
 I-CSCF: Interrogating Call Session Control Function
 S-CSCF: Serving Call Session Control Function

AT&T Proprietary and Confidential

This document and information contained therein is not for use or disclosure outside of AT&T

RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY



ATT-RQ_0000467

An analysis of proprietary backend systems and/or source code may be necessary to fully and accurately describe the functionality of the Accused Instrumentalities with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.